

# BINARY QUARTIC FORMS WITH BOUNDED INVARIANTS AND SMALL GALOIS GROUPS

CINDY (SIN YI) TSANG AND STANLEY YAO XIAO

ABSTRACT. In this paper, we enumerate the  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of integral binary quartic forms which are fixed under substitution by a particular matrix in  $\mathrm{GL}_2(\mathbb{R})$  which is proportional over  $\mathbb{R}$  to an integer matrix. In particular, whenever such a form  $F$  is irreducible, the Galois group of the splitting field of  $F$  is isomorphic to a subgroup of the dihedral group  $\mathcal{D}_4$  of order eight. We also give a new criterion for when the negative Pell's equation  $x^2 - Dy^2 = -1$  is soluble in integers  $x$  and  $y$ .

## CONTENTS

1. Introduction	2
1.1. The main theorems	3
2. Cremona covariants and the automorphism group	8
2.1. Cremona covariants	8
2.2. Relation to Galois groups	9
3. The family $V_{\mathbb{R},f}$ and two new invariants	10
3.1. Two new invariants	11
4. Strategy for the proof of Theorems 1.2, 1.3, and 1.4 (a)	13
4.1. Determinants of the lattices $\Lambda_{f,\alpha}$ and $\Lambda_{f,\beta}$	15
4.2. Reducing to principal forms	17
4.3. Explicit description of the group $O_f(\mathbb{Z})$	18
4.4. Proof of Theorem 1.5	22
5. Parametrizing forms in $V_{\mathbb{R},f}$ of non-zero discriminants	22
5.1. Positive definite case	23
5.2. Indefinite case	25
5.3. Reducible case	28
6. Counting forms of bounded height up to $\mathrm{GL}_2(\mathbb{Z})$ -equivalence	30
6.1. Proof of Theorem 1.2 (a)	31
6.2. Proof of Theorem 1.3 (a)	31
6.3. Proof of Theorem 1.4 (a)	33
7. Estimating the number of forms of square discriminants	36
7.1. Proof of Theorem 1.3 (b)	37
7.2. Proof of Theorems 1.2 and 1.4 (b)	38
8. Estimating the number of reducible forms	39
8.1. Reducibility types	39
8.2. Reducible forms of type 1	41
8.3. Reducible forms of type 2	41
8.4. Proof of Theorem 1.3 (c)	43
8.5. Proof of Theorems 1.2 and 1.4 (c)	44
References	45

## 1. INTRODUCTION

Given a binary quartic form

$$F(x, y) = a_4x^4 + a_3x^3y + a_2x^2y^2 + a_1xy^3 + a_0y^4$$

with real coefficients, we identify  $F$  by its vector of coefficients  $(a_4, a_3, a_2, a_1, a_0) \in \mathbb{R}^5$ . Let  $V_{\mathbb{R}}$  denote the 5-dimensional real vector space of all binary quartic forms with real coefficients and write  $V_{\mathbb{Z}}$  for the lattice in  $V_{\mathbb{R}}$  consisting of points with integer coefficients. In this paper, we shall enumerate integral binary quartic forms with certain Galois structure. Throughout this paper, we will use the convention that the notion of reducibility is always over the field of rational numbers .

Given an irreducible form  $F$ , write  $\text{Gal } F$  for the Galois group of the splitting field of  $F$  over  $\mathbb{Q}$ . We know that  $\text{Gal } F$  is isomorphic to one of the transitive subgroups of the symmetric group  $\mathcal{S}_4$  on four letters: these are  $\mathcal{S}_4$  itself, the alternating group  $\mathcal{A}_4$  on four letters, the dihedral group  $\mathcal{D}_4$  of order eight, the cyclic group  $\mathcal{C}_4$  of order four, or the Klein group  $\mathcal{V}_4$ . We shall say that  $\text{Gal } F$  is *small* if it is not isomorphic to  $\mathcal{S}_4$  or  $\mathcal{A}_4$ . Let  $V_{\mathbb{Z}}^{\text{sm}}$  denote the subset of  $V_{\mathbb{Z}}$  consisting of the irreducible forms having small Galois groups. We are interested in enumerating the  $\text{GL}_2(\mathbb{Z})$ -equivalence classes corresponding to forms with small Galois group . To do so, we need a notion of height.

Given a polynomial  $f(x) = a_nx^n + \cdots + a_1x + a_0$  with integer coefficients, a natural way to measure the size of  $f$  is the so-called *naive* or *box height* given by

$$H_{\text{Box}}(f) = \max_{0 \leq i \leq n} |a_i|.$$

Hilbert's irreducibility theorem implies that as  $X \rightarrow \infty$ , the proportion of degree  $n$  polynomials  $f$  with box height at most  $X$  and whose Galois group  $\text{Gal}(f)$  is isomorphic to the full symmetric group  $\mathcal{S}_n$  tends to 100%. Attempts have been made to make this result *quantitative* as follows. Let  $E_n(X)$  denote the number of degree  $n$  polynomials  $f$  with box height at most  $X$  such that  $\text{Gal}(f)$  is not isomorphic to  $\mathcal{S}_n$ . Gallagher proved in [9] that there exists a positive number  $\gamma$  for which

$$E_n(X) = O(X^{n+1/2}(\log X)^{\gamma}).$$

Zywina improved upon Gallagher's result in [17] by removing the logarithmic factor.

It is clear that  $E_n(X) \gg X^n$ , since polynomials of the shape  $f(x) = a_nx^n + \cdots + a_1x$  with  $a_i \in \mathbb{Z}$  and  $|a_i| \leq X$  for  $i = 1, \dots, n$  are all reducible, and so  $\text{Gal}(f)$  cannot be isomorphic to  $\mathcal{S}_n$ . It remains to be seen whether these reducible polynomials constitute the bulk of the remainder term  $E_n(X)$ .

The notion of box height applies equally well to integral binary forms, but it is not necessarily the correct height to use in this case. A desirable property of any height function is the ability to detect arithmetic complexity. A natural equivalence relation on integral binary forms is  $\text{GL}_2(\mathbb{Z})$ -equivalence under the substitution action. The box height does not detect  $\text{GL}_2(\mathbb{Z})$ -equivalence because two  $\text{GL}_2(\mathbb{Z})$ -equivalent forms may have very different box heights. Since we are interested in counting the  $\text{GL}_2(\mathbb{Z})$ -equivalence classes of the forms in  $V_{\mathbb{Z}}^{\text{sm}}$ , we will need to define a height function which is invariant under  $\text{GL}_2(\mathbb{Z})$ -action. Our height is defined using certain invariants of

binary quartic forms, in an analogous fashion to the approach taken by Bhargava and Shankar in [2].

We note that the problem of enumerating integral binary forms with specific properties up to  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence has a long history. Gauss [10] enumerated positive definite integral binary quadratic forms ordered by their discriminants (see also [13] for the indefinite forms). Davenport [6] [7] enumerated integral binary cubic forms, both of positive and negative discriminants, again by their discriminants. Bhargava, Shankar, and Tsimerman [3] and Thorne and Taniguchi [14] independently improved upon Davenport's work using different methods. The simplest case of enumerating irreducible integral binary forms with *small* Galois group, namely that of enumerating the cubic forms with cyclic Galois groups, was achieved by Bhargava and Shnidman in [4].

Ordering binary quartic forms by discriminant turns out to be more challenging. For binary quadratic forms and binary cubic forms, the discriminant  $\Delta(-)$  is the only rational invariant up to scalar multiples. But for binary quartic forms, there exist two independent invariants  $I(-)$  and  $J(-)$  which together generate the ring of invariants. For  $F \in V_{\mathbb{R}}$ , say

$$F(x, y) = a_4x^4 + a_3x^3y + a_2x^2y^2 + a_1xy^3 + a_0y^4,$$

they are given by the explicit formulae

$$\begin{aligned} I(F) &= 12a_4a_0 - 3a_3a_1 + a_2^2 \\ J(F) &= 72a_4a_2a_0 + 9a_3a_2a_1 - 27a_4a_1^2 - 27a_0a_3^2 - 2a_2^3. \end{aligned}$$

The discriminant of  $F$  is then given by

$$(1.1) \quad \Delta(F) = (4I(F)^3 - J(F)^2)/27,$$

Bhargava and Shankar [2] succeeded in counting binary quartic forms with respect to these two basic invariants, more specifically with respect to the height

$$H_{\mathrm{BS}}(F) = \max\{|I(F)|^3, J(F)^2/4\}.$$

Let  $[-]$  denote  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence class and put

$$N_{\mathrm{BS}}(X) = \#\{[F] : F \in V_{\mathbb{Z}} \text{ and } H_{\mathrm{BS}}(F) \leq X\}.$$

They proved in [2] that for any  $\varepsilon > 0$ , we have

$$N_{\mathrm{BS}}(X) = \frac{44\zeta(2)}{135}X^{5/6} + O_{\varepsilon}(X^{3/4+\varepsilon}).$$

It remains an open problem to count integral binary quartic forms when ordered by discriminant.

**1.1. The main theorems.** In this paper, instead of the usual substitution action, we shall consider the so-called *twisted action* of  $\mathrm{GL}_2(\mathbb{R})$  on a binary form  $\xi(x, y)$  with complex coefficients defined as follows. Given  $T = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}$  in  $\mathrm{GL}_2(\mathbb{R})$ , define

$$(1.2) \quad \xi_T(x, y) = \xi(t_1x + t_2y, t_3x + t_4y) / \sqrt{\det(T)}^{\deg \xi},$$

where  $\sqrt{z}$  denotes the principal square root of any given  $z \in \mathbb{R}$ . Note that (1.2) is only an action up to sign when  $\deg \xi$  is odd, namely  $\xi_{T_1T_2} = \pm(\xi_{T_1})_{T_2}$  in general for

$T_1, T_2 \in \mathrm{GL}_2(\mathbb{R})$ . Also, this twisted action clearly agrees with the substitution action when  $\det(T) = \pm 1$  and  $\deg(\xi)$  is divisible by 4.

For  $F \in V_{\mathbb{R}}$ , write  $\mathrm{Aut}_{\mathbb{R}} F$  for the stabilizer of  $F$  in  $\mathrm{GL}_2(\mathbb{R})$  under (1.2). It is clear that  $\{\lambda I_{2 \times 2} : \lambda \in \mathbb{R}^\times\} \subset \mathrm{Aut}_{\mathbb{R}}(F)$ . When  $F$  has non-zero discriminant, we shall see in Proposition 2.1 below that other elements  $\mathrm{Aut}_{\mathbb{R}}(F)$  are all of the shape  $\begin{pmatrix} \beta & 2\gamma \\ -2\alpha & -\beta \end{pmatrix}$ .

In view of this, we shall introduce the following notation. First, let  $W_{\mathbb{R}}$  denote the 3-dimensional real vector space of all binary quadratic forms with real coefficients and write  $W_{\mathbb{Z}}$  for the lattice in  $W_{\mathbb{R}}$  consisting the forms with integer coefficients. Put

$$W_{\mathbb{R}}^0 = \{f \in W_{\mathbb{R}} \mid \Delta(f) \neq 0\} \text{ and } W_{\mathbb{Z}}^0 = W_{\mathbb{Z}} \cap W_{\mathbb{R}}^0,$$

where  $\Delta(-)$  is the discriminant function. For each  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2 \in W_{\mathbb{R}}^0$ , define

$$(1.3) \quad M_f = \begin{pmatrix} \beta & 2\gamma \\ -2\alpha & -\beta \end{pmatrix}.$$

Further, define

$$V_{\mathbb{R},f} = \{F \in V_{\mathbb{R}} \mid M_f \in \mathrm{Aut}_{\mathbb{R}} F\} \text{ and } V_{\mathbb{Z},f} = V_{\mathbb{R},f} \cap V_{\mathbb{Z}}.$$

In Section 3.1, we shall define two new invariants  $L_f(-)$  and  $K_f(-)$  for the forms in  $V_{\mathbb{R},f}$  having non-zero discriminant. For  $\alpha \neq 0$ , we shall show in Proposition 3.1 below that each  $F \in V_{\mathbb{R},f}$  is determined by the first coefficients,  $A, B$ , and  $C$  say. Then, as we shall compute in Proposition 3.6, the two invariants are given by

$$\begin{aligned} L_f(F) &= -(12\gamma A - 3\beta B + 2\alpha C)/(2\alpha) \\ K_f(F) &= (72\beta^2\gamma A^2 + 9\alpha(\beta^2 + 4\alpha\gamma)B^2 + 8\alpha^3C^2 \\ &\quad - 18\beta(\beta^2 + 4\alpha\gamma)AB + 12\alpha(3\beta^2 - 4\alpha\gamma)AC - 24\alpha^2\beta BC)/(4\alpha^3). \end{aligned}$$

These invariants are *basic* in the sense that the two rational basic invariants  $I(-)$  and  $J(-)$  are polynomials in  $L_f(-)$  and  $K_f(-)$ . Indeed, we shall see in (3.7) that

$$3I(F) = L_f(F)^2 + K_f(F) \text{ and } J(F) = L_f(F)K_f(F)$$

hold. We then deduce from (1.1) that

$$(1.4) \quad \Delta(F) = \left( \frac{L_f(F)^2 + 4K_f(F)}{9} \right) \left( \frac{2L_f(F)^2 - K_f(F)}{9} \right)^2$$

holds as well.

Define the *height of  $F$  associated to  $f$*  by

$$(1.5) \quad H_f(F) = \max\{L_f(F)^2, |K_f(F)|\}.$$

By (3.7), we see that

$$(1.6) \quad H_{\mathrm{BS}}(F) = \max\{27|L_f(F)^2 + K_f(F)|^3, L_f(F)^2 K_f(F)^2/4\},$$

whence there exist absolute constants  $c_1, c_2 > 0$  such that

$$c_1 H_f(F)^3 \leq H_{\mathrm{BS}}(F) \leq c_2 H_f(F)^3.$$

Thus, our height is comparable to that used in [2]. We shall see in Section 3 that there is a natural sense in which the height  $H_f(F)$  is invariant under  $\mathrm{GL}_2(\mathbb{R})$ .

Given an irreducible form  $F \in V_{\mathbb{Z}}$ , it follows from Theorem 2.3 below that  $\mathrm{Gal}(F)$  is small if and only if  $M_f \in \mathrm{Aut}_{\mathbb{R}} F$  for some  $f \in W_{\mathbb{Z}}^0$ . Instead of enumerating the  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of the forms in  $V_{\mathbb{Z}}^{\mathrm{sm}}$ , we may then enumerate those of the irreducible forms in  $V_{\mathbb{Z},f}$  for each  $f \in W_{\mathbb{Z}}^0$ , all of which will have small Galois groups.

Note for any  $f \in W_{\mathbb{Z}}^0$  and  $T \in \mathrm{GL}_2(\mathbb{Z})$ , we have a height-preserving bijection

$$(1.7) \quad V_{\mathbb{R},f_T} \longrightarrow V_{\mathbb{R},f}; \quad F \mapsto F_T$$

by Lemmas 4.6 and 4.7 below. Also, clearly we have  $V_{\mathbb{R},\lambda \cdot f} = V_{\mathbb{R},f}$  for all  $\lambda \in \mathbb{R}^{\times}$ . We then see that it suffices to consider  $V_{\mathbb{Z},f}$  as  $f$  ranges over a set  $\mathcal{F}$  of representatives of the  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of the primitive forms in  $W_{\mathbb{Z},f}^0$ . In particular, we may always take  $f$  to have non-zero  $x^2$ -coefficient, and to be reduced if necessary. Finally, we note that for each  $F \in V_{\mathbb{Z}}^{\mathrm{sm}}$ , as we shall show in Theorem 2.4 below, there are at most three  $f \in \mathcal{F}$  such that  $F$  is  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to a form in  $V_{\mathbb{Z},f}$ .

We state some definitions which will be needed in the statement of our results:

**Definition 1.1.** Let  $f \in W_{\mathbb{Z}}^0$  be given, say  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$ .

- (1) We say that  $f$  is *primitive* if  $\alpha, \beta$ , and  $\gamma$  are coprime.
- (2) For  $f$  positive definite, we say that  $f$  is *reduced* if  $|\beta| \leq \alpha \leq \gamma$ , and  $\beta \geq 0$  when either  $|\beta| = \alpha$  or  $\alpha = \gamma$ .
- (3) For  $f$  reducible, we say that  $f$  is *reduced* if  $\gamma = 0$  and  $0 < \alpha \leq \beta$ .

We shall also need the following notions.

- (4) We say that  $f$  is *ambiguous* if it is  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to a form having the shape  $ax^2 + bxy + cy^2$  with  $a$  dividing  $b$ , and *opaque* if it is  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to a form having the shape  $ax^2 + bxy - ay^2$ .

Note that a form in  $W_{\mathbb{Z}}^0$  can be both ambiguous and opaque. For example, for any  $b \in \mathbb{Z}$ , the form  $x^2 + bxy - y^2$  is ambiguous and opaque via the identity matrix. Also, an opaque form is necessarily indefinite.

In what follows, fix a primitive form

$$f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$$

in  $W_{\mathbb{Z}}^0$  with  $\alpha > 0$ . For  $X > 0$ , define

$$\begin{aligned} V_{\mathbb{Z},f}^0(X) &= \{F \in V_{\mathbb{Z},f} \mid \Delta(F) \neq 0 \text{ and } H_f(F) \leq X\} \\ V_{\mathbb{Z},f}^{\mathrm{red}}(X) &= \{F \in V_{\mathbb{Z},f}^0(X) \mid F \text{ is reducible}\} \\ V_{\mathbb{Z},f}^{\mathrm{sq}}(X) &= \{F \in V_{\mathbb{Z},f}^0(X) \mid \Delta(F) \text{ is a square in } \mathbb{Z}\}. \end{aligned}$$

Further, let  $N_{\mathbb{Z},f}^0(X)$ ,  $N_{\mathbb{Z},f}^{\mathrm{red}}(X)$  and  $N_{\mathbb{Z},f}^{\mathrm{sq}}(X)$ , respectively, denote the number of  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of the forms in  $V_{\mathbb{Z},f}^0(X)$ ,  $V_{\mathbb{Z},f}^{\mathrm{red}}(X)$  and  $V_{\mathbb{Z},f}^{\mathrm{sq}}(X)$ . Our main theorems below give an asymptotic formula for  $N_{\mathbb{Z},f}^0(X)$ , and further state that the quantities  $N_{\mathbb{Z},f}^{\mathrm{sq}}(X)$  and  $N_{\mathbb{Z},f}^{\mathrm{red}}(X)$  only contribute to an error term.

Write  $D_f = |\beta^2 - 4\alpha\gamma|$  for the absolute value of the discriminant of  $f$  and put

$$(1.8) \quad s_f = \begin{cases} 8 & \text{if } \beta \text{ is odd} \\ 1 & \text{if } \beta \text{ is even.} \end{cases}$$

Then, we have:

**Theorem 1.2.** *Let  $f$  be a positive definite binary quadratic form with integer coefficients such that the coefficients of  $f$  are co-prime. Then:*

(a) *We have*

$$N_{\mathbb{Z},f}^0(X) = \frac{1}{s_f r_f} \frac{13\pi}{27D_f^{3/2}} X^{3/2} + O_f(X \log X),$$

where under the assumption that  $f$  is reduced, we have

$$r_f = \begin{cases} 1 & \text{if } f \text{ is not ambiguous} \\ 6 & \text{if } f(x, y) = x^2 + xy + y^2 \\ 2 & \text{otherwise.} \end{cases}$$

(b) *We have*

$$N_{\mathbb{Z},f}^{sq}(X) = O_f(X \log X).$$

(c) *We have*

$$N_{\mathbb{Z},f}^{red}(X) = O_f(X(\log X)^2).$$

**Theorem 1.3.** *Assume that  $f$  is primitive and reducible.*

(a) *We have*

$$N_{\mathbb{Z},f}^0(X) = \frac{1}{s_f r_f} \frac{8}{9D_f^{3/2}} X^{3/2} \log X + O_f(X^{3/2}),$$

where under the assumption that  $f$  is reduced, we have

$$r_f = \begin{cases} 1 & \text{if } \beta \nmid \alpha^2 + 1 \text{ and } \beta \nmid \alpha^2 - 1 \\ 2 & \text{otherwise.} \end{cases}$$

(b) *We have*

$$N_{\mathbb{Z},f}^{sq}(X) = O_f(X(\log X)^3).$$

(c) *We have*

$$N_{\mathbb{Z},f}^{red}(X) = O_f(X(\log X)^3).$$

The case when  $f$  is indefinite and irreducible is more complicated; note that  $D_f > 0$  is not a square in this case. For  $D \in \mathbb{N}$  that is not a square, we shall say that  $D$  is of *negative type* if the negative Pell's equation  $x^2 - Dy^2 = -4$  has an integral solution. Define  $(u_D, v_D)$  to be the smallest positive integral solution to

$$\begin{cases} x^2 - Dy^2 = -4 & \text{if } D \text{ is of negative type} \\ x^2 - Dy^2 = 4 & \text{otherwise.} \end{cases}$$

Also, define  $t_D > 0$  to be such that

$$(1.9) \quad t_D = \log((u_D + v_D \sqrt{D})/2).$$

Then, we have:

**Theorem 1.4.** *Assume that  $f$  is primitive, indefinite, and irreducible.*

(a) We have

$$N_{\mathbb{Z},f}^0(X) = \frac{1}{s_f r_f} \frac{32t_{D_f}}{9D_f^{3/2}} X^{3/2} + O_f(X \log X),$$

where

$$r_f = \begin{cases} 1 & \text{if } f \text{ is neither ambiguous nor opaque} \\ 2 & \text{otherwise.} \end{cases}$$

(b) We have

$$N_{\mathbb{Z},f}^{sq}(X) = O_f(X \log X).$$

(c) We have

$$N_{\mathbb{Z},f}^{red}(X) = O_f(X(\log X)^2).$$

Given  $F \in V_{\mathbb{Z}}$  of non-zero discriminant, the height  $H_f(F)$  is thus far well-defined only when  $f \in W_{\mathbb{Z}}^0$  is fixed. However, when there exists a unique  $f \in W_{\mathbb{Z}}^0$  up to scaling for which  $F \in V_{\mathbb{Z},f}$ , the invariant  $J(-)$  has a unique linear factor over  $\mathbb{Q}$ . Taking that to be  $L(-)$  and setting  $K(-) = J(-)/L(-)$ , we can then define

$$H(F) = \max\{L(F)^2, |K(F)|\}$$

to be *the height of  $F$*  independently of  $f$ . Let  $V_{\mathbb{Z}}^{\dagger}$  denote the subset of  $V_{\mathbb{Z}}$  consisting of all such forms. The above then defines a height function on the set  $V_{\mathbb{Z}}^{\dagger}$ . Let  $[-]$  denote  $\text{GL}_2(\mathbb{Z})$ -equivalence class and put

$$N_{\mathbb{Z}}^{\dagger}(X) = \#\{[F] : F \in V_{\mathbb{Z}}^{\dagger} \text{ and } H(F) \leq X\}.$$

Then, our Theorems 1.2, 1.3, and 1.3 imply that

$$N_{\mathbb{Z}}^{\dagger}(X) \gg X^{3/2} \log X.$$

We suspect that this is actually the correct order of magnitude for the forms in  $V_{\mathbb{Z}}^{\text{sm}}$ . Using (1.6), we then see that the number of  $\text{GL}_2(\mathbb{Z})$ -equivalence classes of  $F \in V_{\mathbb{Z}}^{\text{sm}}$  with  $H_{\text{BS}}(F) \leq X$  should be of order  $X^{1/2} \log X$ , compared to the order  $X^{5/6}$  for the count for all  $F \in V_{\mathbb{Z}}$  with  $H_{\text{BS}}(F) \leq X$ . Using our results and some non-trivial geometry of numbers techniques, we believe that one can obtain an upper bound of

$$N_{\mathbb{Z}}^{\dagger}(X) = O(X^2(\log X)^3),$$

which corresponds to the order  $X^{2/3}(\log X)^3$  in terms of Bhargava-Shankar height. This would improve the bound of  $O_{\varepsilon}(X^{3/4+\varepsilon})$  implied by Bhargava and Shankar's estimation of quartic forms with reducible cubic resolvent in [2].

In a natural way, the set of integral binary quartic forms with small Galois group is comparable to the set of integral binary cubic forms with cyclic Galois group. Both sets contain exactly those irreducible integral forms  $F$  such that  $\text{Aut}_{\mathbb{Q}} F$  is non-trivial, where  $\text{Aut}_{\mathbb{Q}} F$  is defined as in (2.5). In [4], Bhargava and Shnidman enumerated *all* integral binary cubic forms with cyclic Galois group, not just a subset associated to a particular quadratic form. However, our theorems are actually similar to their main result since *all* integral binary cubic forms with cyclic Galois group have Hessian covariant  $\text{GL}_2(\mathbb{Q})$ -equivalent to  $x^2 + xy + y^2$ . In this sense, our theorems above directly generalize their theorem to the quartic case.



As a simple consequence of the proof of Theorem 1.4 (a), we also have the following result relating the notion of ambiguity and opaqueness to the solubility of the negative Pell's equation:

**Theorem 1.5.** *Let  $D = b^2 + 4a^2$ , where  $a, b \in \mathbb{N}$  are coprime and  $D$  is not a square. Then, the negative Pell's equation*

$$x^2 - Dy^2 = -4$$

*is soluble in integers  $x$  and  $y$  if and only if there exists a primitive and integral binary quadratic form such that  $f$  has discriminant  $D$ , and is both ambiguous and opaque.*

## 2. CREMONA COVARIANTS AND THE AUTOMORPHISM GROUP

**2.1. Cremona covariants.** First, we shall recall some results from [16] of the second-named author. We note that the  $\mathrm{GL}_2(\mathbb{R})$ -action on  $V_{\mathbb{R}}$  and hence the notation  $\mathrm{Aut}_{\mathbb{R}} F$  defined in [16] are slightly different from our definitions.

Recall that the ring of invariants for  $V_{\mathbb{R}}$  is generated by two independent invariants, denoted by  $I(-)$  and  $J(-)$ . For  $F \in V_{\mathbb{R}}$ , the *cubic resolvent* of  $F$  is defined by

$$\mathcal{Q}_F(x) = x^3 - 3I(F)x + J(F).$$

It is well-known that for an irreducible form  $F \in V_{\mathbb{Z}}$ , its Galois group  $\mathrm{Gal} F$  is small if and only if  $\mathcal{Q}_F(x)$  has a root in  $\mathbb{Z}$ .

Now, let  $F \in V_{\mathbb{R}}$  be a form having non-zero discriminant and let  $\mathfrak{R}_F$  denote the set consisting of the three distinct roots of  $\mathcal{Q}_F(x)$  in  $\mathbb{C}$ . Elements in  $\mathfrak{R}_F$  may be described explicitly as follows. Let  $T \in \mathrm{GL}_2(\mathbb{Z})$  be any matrix such that  $F_T(x, y)$  has non-zero  $x^4$ -coefficient, and let  $\theta_1, \theta_2, \theta_3, \theta_4 \in \mathbb{C}$  be the distinct roots of  $F_T(x, 1)$  labeled by

$$(2.1) \quad \begin{cases} \theta_1 > \theta_2 > \theta_3 > \theta_4 & \text{if } \theta_1, \theta_2, \theta_3, \theta_4 \in \mathbb{R} \\ \theta_1 > \theta_2, \theta_3 = \overline{\theta_4}, \Im(\theta_3) > 0 & \text{if } \theta_1, \theta_2 \in \mathbb{R} \text{ and } \theta_3, \theta_4 \notin \mathbb{R} \\ \theta_1 = \overline{\theta_2}, \theta_3 = \overline{\theta_4}, \Im(\theta_1) > 0, \Im(\theta_3) < 0 & \text{if } \theta_1, \theta_2, \theta_3, \theta_4 \notin \mathbb{R} \end{cases}$$

as in [1], where  $\Im(z)$  denotes the imaginary part of  $z \in \mathbb{C}$ . Then, an element  $\omega \in \mathfrak{R}_F$  is of the form

$$\omega = 3a_4(\theta_1\theta_{\sigma_\omega(2)} + \theta_{\sigma_\omega(3)}\theta_{\sigma_\omega(4)}), \text{ where } \sigma_\omega \in \{(2)(3)(4), (23)(4), (243)\}.$$

For each  $\omega \in \mathfrak{R}_F$ , define

$$\begin{aligned} \mathfrak{a}_\omega &= a_4(\theta_1 + \theta_{\sigma_\omega(2)} - \theta_{\sigma_\omega(3)} - \theta_{\sigma_\omega(4)}) \\ \mathfrak{b}_\omega &= 2a_4(\theta_{\sigma_\omega(3)}\theta_{\sigma_\omega(4)} - \theta_1\theta_{\sigma_\omega(2)}) \\ \mathfrak{c}_\omega &= a_4(\theta_1\theta_{\sigma_\omega(2)}(\theta_{\sigma_\omega(3)} + \theta_{\sigma_\omega(4)}) - \theta_{\sigma_\omega(3)}\theta_{\sigma_\omega(4)}(\theta_1 + \theta_{\sigma_\omega(2)})). \end{aligned}$$

We then define

$$\mathfrak{C}_{F,\omega}(x, y) = (\mathfrak{C}_{F_T,\omega})_{T^{-1}}(x, y), \text{ where } \mathfrak{C}_{F_T,\omega}(x, y) = \mathfrak{a}_\omega x^2 + \mathfrak{b}_\omega xy + \mathfrak{c}_\omega y^2,$$

called a *Cremona covariant* of  $F$ . As Cremona noted in [5, Section 4], we have

$$(2.2) \quad \mathfrak{C}_{F_T,\omega}(x, y)^2 = ((F_T)_4(x, y) + 4\omega F_T(x, y))/3,$$



where  $(F_T)_4$  is the *Hessian covariant* of  $F_T$  defined as in [16, (2.20)]. This implies that up to sign, the definition of  $\mathfrak{C}_{F,\omega}(x, y)$  does not depend on the choice of  $T \in \mathrm{GL}_2(\mathbb{Z})$  and  $\mathfrak{C}_{F,\omega}(x, y)$  is a covariant of  $F$ . Further, we note that  $\mathfrak{C}_{F,\omega}(x, y)$  has discriminant

$$(2.3) \quad \begin{cases} > 0 & \text{if } \sigma_\omega = (2)(3)(4) \text{ or } (243) \\ < 0 & \text{if } \sigma_\omega = (23)(4), \end{cases}$$

which may easily be verified using (2.1) and [16, (1.28)].

It is clear from (2.1) that for the root  $\omega \in \mathfrak{R}_F$  corresponding to  $(2)(3)(4)$ , we have  $\omega \in \mathbb{R}$  and  $\mathfrak{C}_{F,\omega} \in W_{\mathbb{R}}^0$ . As for the roots  $\omega \in \mathfrak{R}_F$  corresponding to  $(23)(4)$  and  $(243)$ , again using (2.1) and also (2.2), it is not hard to check that

$$(2.4) \quad \begin{cases} \mathfrak{C}_{F,\omega} \in W_{\mathbb{R}}^0 & \text{if } \chi = 4 \\ \lambda \cdot \mathfrak{C}_{F,\omega} \notin W_{\mathbb{R}}^0 \text{ for all } \lambda \in \mathbb{C}^\times & \text{if } \chi = 2 \\ \sqrt{-1} \cdot \mathfrak{C}_{F,\omega} \in W_{\mathbb{R}}^0 & \text{if } \chi = 0, \end{cases}$$

where  $\chi = \chi(F_T)$  denotes the number of real roots of  $F_T(x, 1)$ . Notice that  $\chi = 2$  if and only if  $\Delta(F) < 0$ . In view of this, for each  $\omega \in \mathfrak{R}_F$ , define

$$\mathfrak{C}_{F,\omega}^*(x, y) = \begin{cases} \sqrt{-1} \cdot \mathfrak{C}_{F,\omega}(x, y) & \text{if } \sigma_\omega \in \{(23)(4), (243)\} \text{ and } \chi = 0 \\ \mathfrak{C}_{F,\omega}(x, y) & \text{otherwise.} \end{cases}$$

Then, we have  $\mathfrak{C}_{F,\omega}^* \in W_{\mathbb{R}}^0$  except when  $\sigma_\omega \in \{(23)(4), (243)\}$  and  $\Delta(F) < 0$ .

**Proposition 2.1.** *Let  $F \in V_{\mathbb{R}}$  be a form with non-zero discriminant. Then, a set of representatives of  $\mathrm{Aut}_{\mathbb{R}} F / \{\lambda I_{2 \times 2} : \lambda \in \mathbb{R}^\times\}$  is given by*

$$\begin{cases} \{I_{2 \times 2}\} \sqcup \{M_{\mathfrak{C}_{F,\omega}^*} : \omega \in \mathfrak{R}_F\} & \text{if } \Delta(F) > 0 \\ \{I_{2 \times 2}\} \sqcup \{M_{\mathfrak{C}_{F,\omega_0}^*}\} & \text{if } \Delta(F) < 0, \end{cases}$$

where  $\omega_0 \in \mathfrak{R}_F$  is the root such that  $\sigma_{\omega_0} = (2)(3)(4)$ .

*Proof.* This is essentially [16, Theorem 3.1]. □

We shall also need the following.

**Proposition 2.2.** *Let  $F \in V_{\mathbb{R}}$  be a form with non-zero discriminant. Given  $\omega \in \mathfrak{R}_F$ , there exists  $\lambda \in \mathbb{R}^\times$  such that  $\lambda \cdot \mathfrak{C}_{F,\omega}^*(x, y)$  has integer coefficients if and only if  $\omega \in \mathbb{Z}$ .*

*Proof.* This may be proved using (2.2) (see [16, Lemma 3.6]). □

**2.2. Relation to Galois groups.** Given  $F \in V_{\mathbb{R}}$ , define

$$(2.5) \quad \mathrm{Aut}_{\mathbb{Q}} F = \left\{ \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix} \in \mathrm{Aut}_{\mathbb{R}} F \mid t_1, t_2, t_3, t_4 \in \mathbb{Z} \text{ and } \gcd(t_1, t_2, t_3, t_4) = 1 \right\}.$$

Note that this is different from the  $\mathrm{Aut}_{\mathbb{Q}} F$  defined in [16]. Clearly  $\{\pm I_{2 \times 2}\} \subset \mathrm{Aut}_{\mathbb{Q}} F$ , and we shall say that  $\mathrm{Aut}_{\mathbb{Q}} F$  is *trivial* if  $\mathrm{Aut}_{\mathbb{Q}} F = \{\pm I_{2 \times 2}\}$ . For an irreducible form  $F \in V_{\mathbb{Z}}$ , it turns out that the two groups  $\mathrm{Gal} F$  and  $\mathrm{Aut}_{\mathbb{Q}} F$  are related as follows.

**Theorem 2.3.** *Let  $F \in V_{\mathbb{Z}}$  be an irreducible form. Then, the group  $\mathrm{Gal} F$  is not isomorphic to  $\mathcal{S}_4, \mathcal{A}_4$  if and only if  $\mathrm{Aut}_{\mathbb{Q}} F$  is non-trivial.*

*Proof.* If  $\text{Gal } F$  is small, then  $\omega \in \mathbb{Z}$  for some  $\omega \in \mathfrak{R}_F$ , and we have  $M_{\mathfrak{C}_{F,\omega}^*} \in \text{Aut}_{\mathbb{R}} F$  by Proposition 2.1. Indeed, when  $\Delta(F) > 0$ , this is clear; and when  $\Delta(F) < 0$ , we must have  $\sigma_\omega = (2)(3)(4)$  since  $\mathcal{Q}_F(x)$  has exactly one root in  $\mathbb{R}$  in this case. But  $\mathfrak{C}_{F,\omega}^*(x, y)^2$  has integer coefficients by (2.2), so there exists  $\lambda \in \mathbb{R}^\times$  such that  $\lambda \cdot \mathfrak{C}_{F,\omega}^*(x, y)$  has pairwise coprime integer coefficients. It follows that  $\lambda M_{\mathfrak{C}_{F,\omega}^*} \in \text{Aut}_{\mathbb{Q}} F$ , and this shows that  $\text{Aut}_{\mathbb{Q}} F$  is non-trivial.

Conversely, if  $\text{Aut}_{\mathbb{Q}} F$  is non-trivial, then we have  $\lambda M_{\mathfrak{C}_{F,\omega}^*} \in \text{Aut}_{\mathbb{Q}} F$  for some  $\lambda \in \mathbb{R}^\times$  and  $\omega \in \mathfrak{R}_F$  by Proposition 2.1. This means that  $\lambda \cdot \mathfrak{C}_{F,\omega}^*(x, y)$  has integer coefficients. But then  $\omega \in \mathbb{Z}$  by Proposition 2.2 and so  $\text{Gal } F$  is small.  $\square$

The theorem below shows how Theorems 1.2, 1.3, and 1.4 are related to the problem of enumerating the  $\text{GL}_2(\mathbb{Z})$ -equivalence classes of integral binary quartic forms with small Galois groups.

**Theorem 2.4.** *Let  $\mathcal{F}$  be a set of representatives for the  $\text{GL}_2(\mathbb{Z})$ -equivalence classes of the primitive forms in  $W_{\mathbb{Z}}^0$  and let  $F \in V_{\mathbb{Z}}^{\text{sm}}$ .*

- (a) *If  $\mathcal{Q}_F(x)$  splits over  $\mathbb{Q}$ , then there are exactly two or three  $f \in \mathcal{F}$ , exactly one of which is definite, such that  $F$  is  $\text{GL}_2(\mathbb{Z})$ -equivalent to a form in  $V_{\mathbb{Z},f}$ .*
- (b) *If  $\mathcal{Q}_F(x)$  has exactly one root in  $\mathbb{Q}$ , then there is exactly one  $f \in \mathcal{F}$  such that  $F$  is  $\text{GL}_2(\mathbb{Z})$ -equivalent to a form in  $V_{\mathbb{Z},f}$ .*

*Proof.* Let  $F \in V_{\mathbb{Z}}^{\text{sm}}$  and let  $\omega \in \mathfrak{R}_F$  be any integral root of  $\mathcal{Q}_F(x)$ . As in the proof of Theorem 2.3, we have  $M_{\mathfrak{C}_{F,\omega}^*} \in \text{Aut}_{\mathbb{R}} F$  by Proposition 2.1. By Proposition 2.2, there exists  $\lambda \in \mathbb{R}^\times$  such that  $\lambda \cdot \mathfrak{C}_{F,\omega}^*(x, y)$  has pairwise coprime integer coefficients. Hence, there exists  $f \in \mathcal{F}$  such that  $(\lambda \cdot \mathfrak{C}_{F,\omega}^*)_T = f$  for some  $T \in \text{GL}_2(\mathbb{Z})$ . By Lemmas 4.6 and 4.7 below, we deduce that  $F_T \in V_{\mathbb{Z},f}$ . This, together with (2.3), then implies that if  $\mathcal{Q}_F(x)$  splits over  $\mathbb{Q}$ , then there exist  $f_1, f_2 \in \mathcal{F}$ , one of which is definite and the other indefinite, such that  $F$  is  $\text{GL}_2(\mathbb{Z})$ -equivalent to a form in  $V_{\mathbb{Z},f_i}$  for both  $i \in \{1, 2\}$ . Similarly, if  $\mathcal{Q}_F(x)$  has exactly one root in  $\mathbb{Q}$ , then there is at least one  $f \in \mathcal{F}$  such that  $F$  is  $\text{GL}_2(\mathbb{Z})$ -equivalent to a form in  $V_{\mathbb{Z},f}$ .

Now, let  $f \in \mathcal{F}$  be any element such that  $F_{T^{-1}} \in V_{\mathbb{Z},f}$  for some  $T \in \text{GL}_2(\mathbb{Z})$ . Then, by Lemmas 4.6 and 4.7 below, we have  $F \in V_{\mathbb{Z},f_T}$ . But then Proposition 2.1 implies that  $f_T = \lambda \cdot \mathfrak{C}_{F,\omega}^*$  for some  $\lambda \in \mathbb{R}^\times$  and  $\omega \in \mathfrak{R}_F$ . Note that  $\omega \in \mathbb{Z}$  by Proposition 2.2. Thus, if  $\mathcal{Q}_F(x)$  splits over  $\mathbb{Q}$ , then there are at most three choices for  $f \in \mathcal{F}$ , at most one of which is definite by (2.3). Similarly, if  $\mathcal{Q}_F(x)$  has exactly one root in  $\mathbb{Q}$ , then there is at most one choice for  $f \in \mathcal{F}$ .  $\square$

### 3. THE FAMILY $V_{\mathbb{R},f}$ AND TWO NEW INVARIANTS

In this section, fix a form  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$  in  $W_{\mathbb{R}}^0$ . We have the following explicit descriptions of  $V_{\mathbb{R},f}$  and  $V_{\mathbb{Z},f}$  when  $\alpha \neq 0$  or  $\beta(\beta^2 + 4\alpha\gamma) \neq 0$ . Note that  $V_{\mathbb{R},f}$  is a 3-dimensional subspace of  $V_{\mathbb{R}}$  and  $V_{\mathbb{Z},f}$  is a lattice in  $V_{\mathbb{R},f}$ .

**Proposition 3.1.** *If  $\alpha \neq 0$ , then*

$$(3.1) \quad V_{\mathbb{R},f} = \left\{ \begin{aligned} &Ax^4 + Bx^3y + Cx^2y^2 + \left( \frac{4\beta\gamma A - (\beta^2 + 2\alpha\gamma)B + 2\alpha\beta C}{2\alpha^2} \right) xy^3 \\ &+ \left( \frac{4\gamma(\beta^2 + 2\alpha\gamma)A - \beta(\beta^2 + 4\alpha\gamma)B + 2\alpha\beta^2 C}{8\alpha^3} \right) y^4 : A, B, C \in \mathbb{R} \end{aligned} \right\}.$$

*In particular, when  $f \in W_{\mathbb{Z}}^0$ , the isomorphism  $V_{\mathbb{R},f} \longrightarrow \mathbb{R}^3$  of vector spaces given by*

$$(3.2) \quad Ax^2 + Bx^3y + Cx^2y^2 + (*)xy^3 + (*)y^4 \mapsto (A, B, C)$$

*restricts to a natural identification of  $V_{\mathbb{Z},f}$  with the sublattice  $\Lambda_{f,\alpha}$  in  $\mathbb{Z}^3$  defined by*

$$(3.3) \quad \begin{cases} 4\beta\gamma A - (\beta^2 + 2\alpha\gamma)B + 2\alpha\beta C \equiv 0 & (\text{mod } 2\alpha^2) \\ 4\gamma(\beta^2 + 2\alpha\gamma)A - \beta(\beta^2 + 4\alpha\gamma)B + 2\alpha\beta^2 C \equiv 0 & (\text{mod } 8\alpha^3). \end{cases}$$

*Proof.* For any  $F \in V_{\mathbb{R}}$ , we have  $F \in V_{\mathbb{R},f}$  if and only if  $F(x, y) = F_{M_f}(x, y)$ . Then, a straightforward computation shows that forms in  $V_{\mathbb{R},f}$  indeed take the shape in (3.1). Now, let  $F \in V_{\mathbb{R},f}$  be as in (3.1) corresponding to the tuple  $(A, B, C)$ . It is clear that  $F \in V_{\mathbb{Z},f}$  if and only if  $(A, B, C) \in \mathbb{Z}^3$  such that the  $xy^3, y^4$ -coefficients of  $F$  are also integers, which correspond to the congruence conditions in (3.3).  $\square$

**Proposition 3.2.** *If  $\beta, \beta^2 + 4\alpha\gamma \neq 0$ , then*

$$(3.4) \quad V_{\mathbb{R},f} = \left\{ \begin{aligned} &Ax^4 + \left( \frac{\gamma(4\beta^2 + 8\alpha\gamma)A + 2\alpha\beta^2 B - 8\alpha^3 C}{\beta(\beta^2 + 4\alpha\gamma)} \right) x^3y + Bx^2y^2 \\ &- \left( \frac{8\gamma^3 A - 2\beta^2\gamma B - \alpha(4\beta^2 + 8\alpha\gamma)C}{\beta(\beta^2 + 4\alpha\gamma)} \right) xy^3 + Cy^4 : A, B, C \in \mathbb{R} \end{aligned} \right\}.$$

*In particular, when  $f \in W_{\mathbb{Z}}^0$ , the isomorphism  $V_{\mathbb{R},f} \longrightarrow \mathbb{R}^3$  of vector spaces given by*

$$(3.5) \quad Ax^2 + (*)x^3y + Bx^2y^2 + (*)xy^3 + Cy^4 \mapsto (A, B, C)$$

*restricts to a natural identification of  $V_{\mathbb{Z},f}$  with the sublattice  $\Lambda_{f,\beta}$  in  $\mathbb{Z}^3$  defined by*

$$(3.6) \quad \begin{cases} \gamma(4\beta^2 + 8\alpha\gamma)A + 2\alpha\beta^2 B - 8\alpha^3 C \equiv 0 & (\text{mod } \beta(\beta^2 + 4\alpha\gamma)) \\ 8\gamma^3 A - 2\beta^2\gamma B - \alpha(4\beta^2 + 8\alpha\gamma)C \equiv 0 & (\text{mod } \beta(\beta^2 + 4\alpha\gamma)). \end{cases}$$

*Proof.* Same as the proof of Proposition 3.1  $\square$

**3.1. Two new invariants.** We shall define two new invariants on the forms in  $V_{\mathbb{R},f}$  having non-zero discriminant.

**Lemma 3.3.** *Let  $F \in V_{\mathbb{R}}$  be a form having positive discriminant. Then, the quadratic forms  $\mathfrak{C}_{F,\omega}(x, y)$ , where  $\omega \in \mathfrak{R}_F$ , are pairwise non-proportional over  $\mathbb{C}$ .*

*Proof.* Notice that there exists a matrix  $T \in \text{GL}_2(\mathbb{R})$  such that

$$F_T(x, y) = a_4x^4 + a_2x^2y^2 + a_4y^4.$$

We check that the roots of  $\mathcal{Q}_{F_T}(x)$  are given by

$$\omega_1 = 2a_2, \quad \omega_2 = -6a_4 - a_2, \quad \omega_3 = 6a_4 - a_2.$$

We then deduce from (2.2) that the corresponding Cremona covariants are

$$\begin{aligned}\mathfrak{C}_{F_T, \omega_1}(x, y) &= \pm 2\sqrt{(2a_4 + a_2)(-2a_4 + a_2)}xy \\ \mathfrak{C}_{F_T, \omega_2}(x, y) &= \pm 2\sqrt{-a_4(2a_4 + a_2)}(x^2 + y^2) \\ \mathfrak{C}_{F_T, \omega_3}(x, y) &= \pm 2\sqrt{a_4(2a_4 - a_2)}(x^2 - y^2),\end{aligned}$$

which are pairwise non-proportional over  $\mathbb{C}$ . Since  $\mathfrak{C}_{F_T, \omega}(x, y) = \pm(\mathfrak{C}_{F, \omega})_T(x, y)$  holds for each  $\omega \in \mathfrak{R}_F$  by (2.2), the lemma now follows.  $\square$

Let  $F \in V_{\mathbb{R}, f}$  be a form of non-zero discriminant. Then, we have  $M_f \in \text{Aut}_{\mathbb{R}} F$  by definition, and so  $f = \lambda \cdot \mathfrak{C}_{F, \omega_f(F)}^*$  for some  $\lambda \in \mathbb{R}^\times$  and  $\omega_f(F) \in \mathfrak{R}_F$  by Proposition 2.1. Note that  $\omega_f(F) \in \mathfrak{R}_F$  is unique by (2.4) if  $\Delta(F) < 0$ , and by Lemma 3.3 if  $\Delta(F) > 0$ . Let  $\omega'_f(F), \omega''_f(F) \in \mathfrak{R}_F$  denote the other two roots of  $\mathcal{Q}_F(x)$  and define

$$L_f(F) = \omega_f(F) \text{ and } K_f(F) = -\omega'_f(F)\omega''_f(F).$$

Note that by definition, we have

$$\mathcal{Q}_F(x) = (x - L_f(F))(x^2 + L_f(F)x - K_f(F))$$

By comparing coefficients, it follows that we have the relation

$$(3.7) \quad 3I(F) = L_f(F)^2 + K_f(F) \text{ and } J(F) = L_f(F)K_f(F).$$

Next, we show that  $L_-(-)$  and  $K_-(-)$  are invariant under the action of  $\text{GL}_2(\mathbb{R})$ .

**Proposition 3.4.** *Let  $F \in V_{\mathbb{R}, f}$  be a form of non-zero discriminant. Then, we have*

$$L_{f_T}(F_T) = L_f(F) \text{ and } K_{f_T}(F_T) = K_f(F)$$

for all  $T \in \text{GL}_2(\mathbb{R})$ .

Note that  $F_T \in V_{\mathbb{R}, f_T}$  by Lemmas 4.6 and 4.7 below.

*Proof.* Recall from (2.2) that  $\mathfrak{C}_{F, \omega}(x, y)$  is a covariant of  $F$  up to sign for each  $\omega \in \mathfrak{R}_F$ . In particular, if  $f(x, y) = \lambda \cdot \mathfrak{C}_{F, \omega_f(F)}(x, y)$ , then  $f_T(x, y) = \pm \lambda \cdot \mathfrak{C}_{F_T, \omega_f(F)}(x, y)$ . Then, by definition  $\omega_{f_T}(F_T) = \omega_f(F)$ , whence  $L_{f_T}(F_T) = L_f(F)$ . Since  $I(F_T) = I(F)$ , we have  $K_{f_T}(F_T) = K_f(F)$  as well by the first equality in (3.7).  $\square$

We shall also make the following observation.

**Proposition 3.5.** *Assume that  $f \in W_{\mathbb{Z}}^0$ . Then, for all  $F \in V_{\mathbb{Z}, f}$  of non-zero discriminant, we have  $L_f(F), K_f(F), (L_f(F)^2 + 4K_f(F))/9, (2L_f(F)^2 - K_f(F))/9 \in \mathbb{Z}$ .*

*Proof.* Notice that  $f(x, y) = \lambda \cdot \mathfrak{C}_{F, L_f(F)}(x, y)$  for some  $\lambda \in \mathbb{R}^\times$  by definition. Since  $f$  has integer coefficients, we have  $L_f(F) \in \mathbb{Z}$  by Proposition 2.2. Since  $I(F) \in \mathbb{Z}$ , we have  $K_f(F) \in \mathbb{Z}$  as well by the first equation in (3.7). Next, observe that

$$\begin{aligned}I(F) + K_f(F) &= (L_f(F)^2 + 4K_f(F))/3 \\ 2I(F) - K_f(F) &= (2L_f(F)^2 - K_f(F))/3,\end{aligned}$$

which are both integers. Since  $\Delta(F) \in \mathbb{Z}$ , we then deduce from (1.4) one of the above expressions is divisible by 3. But again by (3.7), we have

$$I(F) = (L_f(F)^2 + 4K_f(F))/9 + (2L_f(F)^2 - K_f(F))/9,$$

so in fact both expressions are divisible by 3. This proves the claim.  $\square$

Finally, we give explicit formulae for  $L_f(-)$  and  $K_f(-)$  in two special cases.

**Proposition 3.6.** *Assume that  $\alpha \neq 0$ . Then, for all  $F \in V_{\mathbb{R},f}$  as in (3.1) of non-zero discriminant, we have*

$$\begin{aligned} L_f(F) &= -(12\gamma A - 3\beta B + 2\alpha C)/(2\alpha) \\ K_f(F) &= (72\beta^2\gamma A^2 + 9\alpha(\beta^2 + 4\alpha\gamma)B^2 + 8\alpha^3C^2 \\ &\quad - 18\beta(\beta^2 + 4\alpha\gamma)AB + 12\alpha(3\beta^2 - 4\alpha\gamma)AC - 24\alpha^2\beta BC)/(4\alpha^3). \end{aligned}$$

Moreover, we have

$$\frac{4(L_f(F)^2 + 4K_f(F))}{9} = \frac{L_{f,1}(F)^2 - (\beta^2 - 4\alpha\gamma)L_{f,2}(F)^2}{\alpha^4},$$

where

$$L_{f,1}(F) = 4(\beta^2 - \alpha\gamma)A - 3\alpha\beta B + 2\alpha^2C \text{ and } L_{f,2}(F) = 2(2\beta A - \alpha B).$$

*Proof.* This may be verified by explicit calculation.  $\square$

**Proposition 3.7.** *Assume that  $\gamma = 0$  and  $\beta \neq 0$ . Then, for all  $F \in V_{\mathbb{R},f}$  as in (3.4) of non-zero discriminant, we have*

$$\begin{aligned} L_f(F) &= (2\beta^2B - 12\alpha^2C)/\beta^2 \\ K_f(F) &= (-\beta^4B^2 + 144\alpha^4C^2 + 36\beta^4AC - 24\alpha^2\beta^2BC)/\beta^4. \end{aligned}$$

Moreover, we have

$$\frac{4(L_f(F)^2 + 4K_f(F))}{9} = \frac{8C}{\beta^2} \left( 8\beta^2A - 8\alpha^2B + \frac{40\alpha^4}{\beta^2}C \right).$$

*Proof.* This may be verified by explicit computation.  $\square$

#### 4. STRATEGY FOR THE PROOF OF THEOREMS 1.2, 1.3, AND 1.4 (A)

The key to the proof of the Theorems 1.2 to 1.4 is the following proposition.

**Proposition 4.1** (Davenport's lemma). *Let  $\mathcal{R}$  be a bounded, semi-algebraic multi-set in  $\mathbb{R}^n$  having maximum multiplicity  $m$  and that is defined by at most  $k$  polynomial inequalities, each having degree at most  $\ell$ . Then the number of integral lattice points (counted with multiplicity) contained in the region  $\mathcal{R}$  is*

$$\text{Vol}(\mathcal{R}) + O(\max\{\text{Vol}(\overline{\mathcal{R}}), 1\}),$$

where  $\text{Vol}(\overline{\mathcal{R}})$  denotes the greatest  $d$ -dimensional volume of any projection of  $\mathcal{R}$  onto a coordinate subspace by equating  $n - d$  coordinates to zero, with  $1 \leq d \leq n - 1$ . The implied constant in the second summand depends only on  $n, m, k, \ell$ .

*Proof.* See [2].  $\square$

Throughout this section, let  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$  be a form in  $W_{\mathbb{Z}}^0$  with  $\alpha > 0$ . If  $f$  is irreducible, then we shall identify  $V_{\mathbb{R},f}$  with  $\mathbb{R}^3$  via the isomorphism (3.2). If  $f$  is reducible, in which case we may assume that  $\beta, \beta^2 + 4\alpha\gamma \neq 0$ , then we shall identify  $V_{\mathbb{R},f}$  with  $\mathbb{R}^3$  via the isomorphism (3.5).

Next, define

$$V_{\mathbb{R},f}^0 = \{F \in V_{\mathbb{R},f} \mid \Delta(F) \neq 0\} \text{ and } V_{\mathbb{Z},f}^0 = V_{\mathbb{R},f}^0 \cap V_{\mathbb{Z},f}.$$

For  $X > 0$ , further put

$$V_{\mathbb{R},f}^0(X) = \{F \in V_{\mathbb{R},f}^0 \mid H_f(F) \leq X\}.$$

We shall define a bounded semi-algebraic subset  $\mathcal{S}_f(X)$  of  $V_{\mathbb{R},f}^0(X)$  such that:

- (1) the number of polynomial inequalities defining the set  $\mathcal{S}_f(X)$  and the degrees of these polynomials are absolutely bounded;
- (2) there exists at least one representative in  $\mathcal{S}_f(X)$  for each  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence class of the forms in  $V_{\mathbb{Z},f}^0(X)$ ;
- (3) there exists a constant  $r_f \in \mathbb{N}$  such that for each  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence class of the forms in  $V_{\mathbb{Z},f}^0(X) \setminus V_{\mathbb{Z},f}^{\mathrm{sq}}(X)$ , there are exactly  $r_f$  representatives in  $\mathcal{S}_f(X)$ .

Let  $\mathcal{L}_{f,*} : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  be any linear transformation which sends  $\Lambda_{f,*}$  to  $\mathbb{Z}^3$ , where  $\Lambda_{f,*}$  is the lattice in  $\mathbb{R}^3$  defined by (3.3) or (3.6), and

$$* = \begin{cases} \alpha & \text{if } f \text{ is irreducible} \\ \beta & \text{if } f \text{ is reducible.} \end{cases}$$

We shall apply Proposition 4.1 to the set  $\mathcal{R}_f(X) = \mathcal{L}_{f,*}(\mathcal{S}_f(X))$ . Notice that integral points in  $\mathcal{R}_f(X)$  correspond to integral forms in  $\mathcal{S}_f(X)$ .

Now, observe that we have

$$\mathrm{Vol}(\mathcal{R}_f(X)) = \mathrm{Vol}(\mathcal{S}_f(X)) \det(\mathcal{L}_{f,*}) = \mathrm{Vol}(\mathcal{S}_f(X)) \det(\Lambda_{f,*})^{-1}.$$

In the proof of Theorems 1.2, 1.3, and 1.4 (a), we shall compute that

$$\mathrm{Vol}(\overline{\mathcal{R}_f(X)}) = \begin{cases} O_f(X) & \text{if } f \text{ is irreducible} \\ O_f(X^{3/2}) & \text{if } f \text{ is reducible.} \end{cases}$$

In the proof of Theorems 1.2, 1.3, and 1.4 (b), we shall also see that the number of integral forms in  $\mathcal{S}_f(X)$  having square discriminants is bounded above by

$$\begin{cases} O_f(X \log X) & \text{if } f \text{ is irreducible} \\ O_f(X(\log X)^3) & \text{if } f \text{ is reducible.} \end{cases}$$

By removing the forms of square discriminants in from  $\mathcal{S}_f(X)$ , we deduce that

$$(4.1) \quad N_{\mathbb{Z},f}^0(X) = \begin{cases} \frac{1}{r_f} \frac{\mathrm{Vol}(\mathcal{S}_f(X))}{\det(\Lambda_{f,*})} + O_f(X \log X) & \text{if } f \text{ is irreducible} \\ \frac{1}{r_f} \frac{\mathrm{Vol}(\mathcal{S}_f(X))}{\det(\Lambda_{f,*})} + O_f(X^{3/2}) & \text{if } f \text{ is reducible.} \end{cases}$$

We shall compute  $\det(\Lambda_{f,*})$  in the next section. To define  $\mathcal{S}_f(X)$ , we shall parametrize the set  $V_{\mathbb{R},f}^0$  in terms of the  $L_f$ - and  $K_f$ -invariants defined in Section 3.1, as well as a parameter  $t$  that arises from the group

$$O_f(\mathbb{R}) = \{T \in \mathrm{GL}_2(\mathbb{R}) \mid \det(T) = \pm 1 \text{ and } f_T = \pm f\}.$$

In Section 4.2, we shall explain why essentially it suffices to consider the forms  $x^2 + y^2$  and  $x^2 - y^2$ . In Section 4.3, we shall give an explicit description of the subgroup

$$O_f(\mathbb{Z}) = O_f(\mathbb{R}) \cap \mathrm{GL}_2(\mathbb{Z}),$$



which is needed to determine the value of  $r_f$ . By Corollary 4.9 below, we know that

$$(4.2) \quad r_f = \#\{G \in \mathcal{S}_f(X) \mid G = F_T \text{ for some } T \in O_f(\mathbb{Z})\}$$

for all integral forms  $F \in \mathcal{S}_f(X)$  having non-square discriminant.

**4.1. Determinants of the lattices  $\Lambda_{f,\alpha}$  and  $\Lambda_{f,\beta}$ .** Provided that  $\beta, \beta^2 + 4\alpha\gamma \neq 0$ , the transition matrix from the basis of  $V_{\mathbb{R},f}$  given by (3.2) to that given by (3.5) is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ * & -\mathcal{B} & * \end{pmatrix}, \text{ where } \mathcal{B} = \frac{\beta(\beta^2 + 4\alpha\gamma)}{8\alpha^3}.$$

It has determinant  $\mathcal{B}$  and maps  $\Lambda_{f,\alpha}$  onto  $\Lambda_{f,\beta}$ . It follows that  $\det(\Lambda_{f,\beta}) = \mathcal{B} \det(\Lambda_{f,\alpha})$ , whence it suffice to compute  $\det(\Lambda_{f,\alpha})$ . To that end, recall that  $\Lambda_{f,\alpha}$  is defined by

$$\mathcal{A}_1 \equiv 0 \pmod{2\alpha^2} \text{ and } \mathcal{A}_2 \equiv 0 \pmod{8\alpha^3},$$

where

$$\begin{aligned} \mathcal{A}_1 &= 4\beta\gamma A - (\beta^2 + 2\alpha\gamma)B + 2\alpha\beta C \\ \mathcal{A}_2 &= 4\gamma(\beta^2 + 2\alpha\gamma)A - \beta(\beta^2 + 4\alpha\gamma)B + 2\alpha\beta^2 C. \end{aligned}$$

Observe that  $\Lambda_{f,\alpha} = \Lambda_{f/d,\alpha/d}$ , where  $d = \gcd(\alpha, \beta, \gamma)$ . Hence, in what follows, without loss of generality, we may assume that  $f$  is primitive. As in (1.8), define  $s_f = 8$  if  $\beta$  is odd and  $s_f = 1$  if  $\beta$  is even. We shall prove:

**Proposition 4.2.** *We have  $\det(\Lambda_{f,\alpha}) = s_f \alpha^3$ , and  $\det(\Lambda_{f,\beta}) = s_f \beta(\beta^2 + 4\alpha\gamma)/8$ .*

*Proof.* By the above discussion, it is enough to show that  $\det(\Lambda_{f,\alpha}) = s_f \alpha^3$ . If  $\beta = 0$ , then  $\alpha$  and  $\gamma$  are coprime. We then easily see that  $\Lambda_{f,\alpha}$  is defined by

$$A \equiv 0 \pmod{\alpha^2} \text{ and } B \equiv 0 \pmod{\alpha}.$$

Hence, a  $\mathbb{Z}$ -basis for  $\Lambda_{f,\alpha}$  is given by  $\{(\alpha^2, 0, 0), (0, \alpha, 0), (0, 0, 1)\}$  and  $\det(\Lambda_{f,\alpha}) = \alpha^3$ . Similarly, if  $\gamma = 0$ , then  $\alpha$  and  $\beta$  are coprime. We easily check that  $\Lambda_{f,\alpha}$  is defined by

$$B \equiv 0 \pmod{s_f^{1/3} \alpha} \text{ and } (\beta B - 2\alpha C)/(2\alpha) \equiv 0 \pmod{s_f^{2/3} \alpha^2}.$$

Thus, a  $\mathbb{Z}$ -basis for  $\Lambda_{f,\alpha}$  is given by  $\{(1, 0, 0), s_f^{1/2}(0, \alpha, \beta/2), s_f^{2/3}(0, 0, \alpha^2)\}$ , and so we have  $\det(\Lambda_{f,\alpha}) = s_f \alpha^3$ . Finally, if  $\beta, \gamma \neq 0$ , then we use the fact that

$$\det(\Lambda_{f,\alpha}) = \prod_{p|2\alpha} \det(\Lambda_{f,\alpha}^{(p)}),$$

where  $\Lambda_{f,\alpha}^{(p)}$  denotes the  $\mathbb{Z}_p$ -lattice obtained from  $\Lambda_{f,\alpha}$  by extending scalars to  $\mathbb{Z}_p$ . Now, given a prime  $p \mid 2\alpha$ , let  $p^k$  be the exact power of  $p$  dividing  $\alpha$ . From Lemmas 4.3, 4.4, and 4.5 below, we know that  $\det(\Lambda_{f,\alpha}^{(2)}) = s_f 2^{3k}$  and  $\det(\Lambda_{f,\alpha}^{(p)}) = p^{3k}$  for  $p \neq 2$ . Hence, indeed  $\det(\Lambda_{f,\alpha}) = s_f \alpha^3$ , as desired.  $\square$

In what follows, assume that  $\beta, \gamma \neq 0$ , and fix a prime  $p$  dividing  $2\alpha$ . Also, write

$$\alpha = p^k a \text{ and } \beta = p^\ell b,$$

where  $a$  and  $b$  are non-zero integers coprime to  $p$ . Notice that  $k \geq 1$  when  $p$  is odd. Then, the lattice  $\Lambda_{f,\alpha}^{(p)}$  is defined by the congruences

$$(4.3) \quad \mathcal{A}_1 \equiv 0 \pmod{p^{2k+\varepsilon}} \text{ and } \mathcal{A}_2 \equiv 0 \pmod{p^{3k+3\varepsilon}},$$



where  $\varepsilon = 1$  if  $p = 2$  and  $\varepsilon = 0$  if  $p$  is odd. We shall rewrite

$$(4.4) \quad \begin{aligned} \mathcal{A}_1 &= p^\ell b(4\gamma A - p^\ell bB) - 2p^k a\gamma B + 2p^{k+\ell} abC \\ \mathcal{A}_2 &= (p^{2\ell} b^2 + 4p^k a\gamma)(4\gamma A - p^\ell bB) - 8p^k a\gamma^2 A + 2p^{k+2\ell} ab^2 C. \end{aligned}$$

Also, observe that we have the relation

$$(4.5) \quad \mathcal{A}_2 - p^\ell b\mathcal{A}_1 = 2p^k a\gamma(4\gamma A - p^\ell bB).$$

**Lemma 4.3.** *If  $\ell = 0$ , then  $\det(\Lambda_{f,\alpha}^{(p)}) = p^{3k+3\varepsilon}$ .*

*Proof.* If  $\ell = 0$ , then by (4.5) the congruence  $\mathcal{A}_2 \equiv 0 \pmod{p^{3k+3\varepsilon}}$  is equivalent to

$$4\gamma A - bB \equiv 0 \pmod{p^{k+\varepsilon}} \text{ and } \mathcal{A}_2/p^{k+\varepsilon} \equiv 0 \pmod{p^{2k+2\varepsilon}}.$$

We then see from (4.5) that  $\Lambda_{f,\alpha}^{(p)}$  is defined solely by  $\mathcal{A}_2 \equiv 0 \pmod{p^{3k+3\varepsilon}}$ . A  $\mathbb{Z}_p$ -basis for  $\Lambda_{f,\alpha}^{(p)}$  is given by  $\{(b^2, 4b\gamma, 4\gamma^2), (0, 2abp^k, b^2 + 4p^k a\gamma), (0, 0, p^{2k+2\varepsilon})\}$ . Since  $a$  and  $b$  are units in  $\mathbb{Z}_p$ , we see that indeed  $\det(\Lambda_{f,\alpha}^{(p)}) = p^{3k+3\varepsilon}$ .  $\square$

**Lemma 4.4.** *If  $\ell \geq 1$ , and either  $k = 0$  or  $\ell \geq k + 2\varepsilon$ , then  $\det(\Lambda_{f,\alpha}^{(p)}) = p^{3k}$ .*

*Proof.* If  $\ell \geq 1$  and  $k = 0$ , then  $p = 2$  and  $\Lambda_{f,\alpha}^{(2)} = \mathbb{Z}_p^3$  has determinant one. If  $k, \ell \geq 1$ , then  $p$  divides both  $\alpha$  and  $\beta$ , and so  $p$  does not divide  $\gamma$ . If further  $\ell \geq k + 2\varepsilon$ , then we claim that  $\Lambda_{f,\alpha}^{(p)}$  is defined by

$$(4.6) \quad A \equiv 0 \pmod{p^{2k}} \text{ and } B \equiv 0 \pmod{p^k}.$$

Indeed, it is straightforward to verify that (4.6) implies (4.3). Conversely, when (4.3) holds, reducing (4.5) mod  $p^{3k+3\varepsilon}$  and rewriting  $\mathcal{A}_1 \equiv 0 \pmod{p^{2k+\varepsilon}}$ , respectively, yield

$$4\gamma A - p^\ell bB \equiv 0 \pmod{p^{2k+2\varepsilon}} \text{ and } 4p^\ell b\gamma A - 2p^k a\gamma B \equiv 0 \pmod{p^{2k+\varepsilon}}.$$

The first congruence gives  $A \equiv 0 \pmod{p^k}$ . We then see from the second congruence that  $B \equiv 0 \pmod{p^k}$ , and again from the first congruence that  $A \equiv 0 \pmod{p^{2k}}$ . So, a  $\mathbb{Z}_p$ -basis for  $\Lambda_{f,\alpha}^{(p)}$  is given by  $\{(p^{2k}, 0, 0), (0, p^k, 0), (0, 0, 1)\}$  and  $\det(\Lambda_{f,\alpha}^{(p)}) = p^{3k}$ .  $\square$

**Lemma 4.5.** *If  $1 \leq k, \ell \leq k + \varepsilon$ , then  $\det(\Lambda_{f,\alpha}^{(p)}) = p^{3k}$ .*

*Proof.* If  $k, \ell \geq 1$ , then  $p$  divides both  $\alpha$  and  $\beta$ , whence  $p$  does not divide  $\gamma$ . If further  $\ell \leq k + \varepsilon$ , then we claim that  $\Lambda_{f,\alpha}^{(p)}$  is defined by

$$(4.7) \quad \begin{cases} A \equiv 0 & (\text{mod } p^{2\ell-2\varepsilon}) \\ B \equiv 0 & (\text{mod } p^{\ell-\varepsilon}) \\ (4\gamma A - p^\ell bB)/p^{2\ell-\varepsilon} \equiv 0 & (\text{mod } p^{k-\ell+\varepsilon}) \\ \mathcal{A}_2/p^{k+2\ell+\varepsilon} \equiv 0 & (\text{mod } p^{2k-2\ell+2\varepsilon}). \end{cases}$$

Using the relation (4.5), it is easy to check that (4.7) implies (4.3). Conversely, when (4.3) holds, reducing (4.5) mod  $p^{2k+\ell+\varepsilon}$  yields

$$4\gamma A - p^\ell bB \equiv 0 \pmod{p^{k+\ell}}.$$

Since  $\mathcal{A}_1 \equiv 0 \pmod{p^{k+\ell}}$ , the above and (4.5) imply that  $B \equiv 0 \pmod{p^{\ell-\varepsilon}}$ . Similarly, since  $\mathcal{A}_2 \equiv 0 \pmod{p^{k+2\ell+\varepsilon}}$ , the above and (4.5) imply that  $A \equiv 0 \pmod{p^{2\ell-2\varepsilon}}$ . We

then see that both  $(4\gamma A - p^\ell bB)/p^{2\ell-\varepsilon}$  and  $\mathcal{A}_2/p^{k+2\ell+\varepsilon}$  are integers, and (4.7) indeed holds. Hence, a  $\mathbb{Z}_p$ -basis for  $\Lambda_{f,\alpha}^{(p)}$  is given by

$$\{(p^{2\ell-2\varepsilon}b^2, 4p^{\ell-2\varepsilon}b\gamma, 4p^{-2\varepsilon}\gamma^2), (0, 2abp^{k-\varepsilon}, p^{\ell-\varepsilon}b^2 + 4p^{k-\ell-\varepsilon}a\gamma), (0, 0, p^{2k-2\ell+2\varepsilon})\}.$$

Since  $a$  and  $b$  are units in  $\mathbb{Z}_p$ , we see that  $\det(\Lambda_{f,\alpha}^{(p)}) = p^{3k}$ , as claimed.  $\square$

**4.2. Reducing to principal forms.** We first note the following:

**Lemma 4.6.** *For all  $F \in V_{\mathbb{R}}$  and  $T \in \mathrm{GL}_2(\mathbb{R})$ , we have  $\mathrm{Aut}_{\mathbb{R}} F_T = T^{-1}(\mathrm{Aut}_{\mathbb{R}} F)T$ .*

*Proof.* This is clear (cf. [16, Lemma 2.1]).  $\square$

**Lemma 4.7.** *Let  $f_1, f_2 \in W_{\mathbb{R}}^0$  and  $T \in \mathrm{GL}_2(\mathbb{R})$ . For all  $\lambda \in \mathbb{R}^\times$ , we have  $\lambda \cdot f_2 = (f_1)_T$  if and only if the equality  $\lambda \cdot M_{f_2} = T^{-1}M_{f_1}T$  holds (recall the notation (1.3)).*

*Proof.* For  $i = 1, 2$ , write  $f_i(x, y) = \alpha_i x^2 + \beta_i xy + \gamma_i y^2$  and observe that

$$M_{f_i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 2\alpha_i & \beta_i \\ \beta_i & 2\gamma_i \end{pmatrix}.$$

The equality  $\lambda \cdot M_{f_2} = T^{-1}M_{f_1}T$  is then equivalent to

$$\lambda \cdot \begin{pmatrix} 2\alpha_2 & \beta_2 \\ \beta_2 & 2\gamma_2 \end{pmatrix} = \frac{1}{\det(T)} \cdot T^t \begin{pmatrix} 2\alpha_1 & \beta_1 \\ \beta_1 & 2\gamma_1 \end{pmatrix} T.$$

It is not hard to check that the above in turn is equivalent to  $\lambda \cdot f_2 = (f_1)_T$ .  $\square$

Let  $D$  be the absolute value of the discriminant of  $f$  and put  $\delta = D/4$ . Also, let

$$(4.8) \quad f_0(x, y) = \begin{cases} x^2 + y^2 & \text{if } f \text{ is positive definite} \\ x^2 - y^2 & \text{if } f \text{ is indefinite} \end{cases}$$

and define the matrix

$$(4.9) \quad T_f = \begin{pmatrix} \delta^{-1/4} & 0 \\ 0 & \delta^{1/4} \end{pmatrix} \cdot \frac{1}{2\sqrt{\alpha}} \begin{pmatrix} 2\alpha & \beta \\ 0 & 2 \end{pmatrix}.$$

Observe that  $\det(T_f) = 1$  and that  $\delta^{-1/2} \cdot f = (f_0)_{T_f}$ . Then, the map

$$(4.10) \quad \Psi_f : V_{\mathbb{R}, f_0} \longrightarrow V_{\mathbb{R}, f}; \quad \Psi_f(F) = F_{T_f}$$

is a well-defined bijection by Lemmas 4.6 and 4.7.

Now, recall from (3.1) that an element in  $V_{\mathbb{R}, f_0}$  is of the form

$$F(x, y) = a_4 x^4 + a_3 x^3 y + a_2 x^2 y^2 \pm a_3 x y^3 + a_4 y^4.$$

A straightforward computation yields

$$F_{T_f}(x, y) = Ax^4 + Bx^3y + Cx^2y^2 + (*)xy^3 + (*)y^4,$$

where

$$(4.11) \quad A = \frac{\alpha^2 a_4}{\delta}, \quad B = \frac{2\alpha\beta a_4}{\delta} + \frac{\alpha a_3}{\sqrt{\delta}}, \quad C = \frac{3\beta^2 a_4}{2\delta} + \frac{3\beta a_3}{2\sqrt{\delta}} + a_2.$$

So, identifying  $V_{\mathbb{R}, f_0}$  and  $V_{\mathbb{R}, f}$  with  $\mathbb{R}^3$  via (3.2), the matrix of  $\Psi_f$  is lower triangular with diagonal entries  $\alpha^2 \delta^{-1}$ ,  $\alpha \delta^{-1/2}$ , and 1. In particular, we have  $\det(\Psi_f) = \alpha^3 \delta^{-3/2}$ .

**4.3. Explicit description of the group  $O_f(\mathbb{Z})$ .** The following lemma and corollary are why we need to avoid the forms in  $V_{\mathbb{Z},f}^0(X)$  of square discriminants, and also why understanding  $O_f(\mathbb{Z})$  will help us determine the value of  $r_f$  given in (4.2).

**Lemma 4.8.** *Let  $f_1, f_2 \in W_{\mathbb{Z}}^0$  and  $T \in \mathrm{GL}_2(\mathbb{Z})$ . If there exists a form  $F \in V_{\mathbb{Z},f_1}^0$  with non-square discriminant such that  $F_T \in V_{\mathbb{Z},f_2}^0$ , then  $\lambda \cdot f_2 = (f_1)_T$  for some  $\lambda \in \mathbb{R}^\times$ .*

*Proof.* Let  $F \in V_{\mathbb{Z},f_1}^0$  be such a form. Notice that  $T^{-1}M_{f_1}T \in \mathrm{Aut}_{\mathbb{R}} F_T$  by Lemma 4.6, and that  $M_{f_2} \in \mathrm{Aut}_{\mathbb{R}} F_T$  because  $F_T \in V_{\mathbb{Z},f_2}^0$ . Recall the notation in Section 2.1. Then, by Proposition 2.1, we know that

$$T^{-1}M_{f_1}T = \lambda_1 M_{\mathfrak{C}_{F,\omega_1}^*} \text{ and } M_{f_2} = \lambda_2 M_{\mathfrak{C}_{F,\omega_2}^*},$$

where  $\lambda_1, \lambda_2 \in \mathbb{R}^\times$  and  $\omega_1, \omega_2$  are roots of  $\mathcal{Q}_F(x)$ . The above is equivalent to

$$\lambda_1 \cdot \mathfrak{C}_{F,\omega_1}^*(x, y) = (f_1)_T(x, y) \text{ and } \lambda_2 \cdot \mathfrak{C}_{F,\omega_2}^*(x, y) = f_2(x, y)$$

by Lemma 4.7. Note that  $\omega_1, \omega_2 \in \mathbb{Z}$  by Proposition 2.2. Suppose that  $\omega_1 \neq \omega_2$ . This implies that  $\mathcal{Q}_F(x)$  has three distinct roots in  $\mathbb{Z}$  and hence its discriminant  $\Delta(\mathcal{Q}_F(x))$  is a square in  $\mathbb{Z}$ . But  $\Delta(F) = 27^2 \Delta(\mathcal{Q}_F(x))$ , so then  $\Delta(F)$  is a square in  $\mathbb{Z}$ , which is a contradiction. Hence, we have  $\omega_1 = \omega_2$ , in which case  $\lambda \cdot f_2 = (f_1)_T$  for  $\lambda = \lambda_1 \lambda_2^{-1}$ .  $\square$

**Corollary 4.9.** *Given a form  $F \in V_{\mathbb{Z},f}^0$  of non-square discriminant and  $T \in \mathrm{GL}_2(\mathbb{Z})$ , we have  $F_T \in V_{\mathbb{Z},f}^0$  if and only if  $T \in O_f(\mathbb{Z})$ . Moreover, for  $T \in O_f(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}$ , we have  $F_T = F$  precisely when  $T = \lambda \begin{pmatrix} \beta & 2\gamma \\ -2\alpha & -\beta \end{pmatrix}$  for some  $\lambda \in \mathbb{R}^\times$ .*

*Proof.* If  $F_T \in V_{\mathbb{Z},f}^0$ , then  $\lambda \cdot f = f_T$  for some  $\lambda \in \mathbb{R}^\times$  by Lemma 4.8. Clearly  $\lambda = \pm 1$ , whence  $T \in O_f(\mathbb{Z})$ . If  $T \in O_f(\mathbb{Z})$ , then  $F_T \in V_{\mathbb{Z},f}^0$  by Lemmas 4.6 and 4.7.

Now, suppose that  $T \in O_f(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}$ . If  $F_T = F$ , then  $T$  is of the shape  $\begin{pmatrix} b & 2c \\ -2a & -b \end{pmatrix}$  by Proposition 2.1. But then  $F \in V_{\mathbb{Z},g}^0$  for  $g(x, y) = ax^2 + bxy + cy^2$ , and so  $\lambda \cdot g = f$ , meaning that  $T = \lambda \begin{pmatrix} \beta & 2\gamma \\ -2\alpha & -\beta \end{pmatrix}$ , for some  $\lambda \in \mathbb{R}^\times$  by Lemma 4.8. The converse follows directly from Proposition 2.1.  $\square$

Now, in order to explicitly describe the elements in  $O_f(\mathbb{Z})$ , let  $f_0(x, y)$  be given as in (4.8). For  $f_0(x, y) = x^2 + y^2$ , the group  $O_{f_0}(\mathbb{R})$  is the usual orthogonal group

$$(4.12) \quad O(2) = \left\{ \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix} : t \in \mathbb{R} \right\} \cup \left\{ \begin{pmatrix} \cos t & \sin t \\ \sin t & -\cos t \end{pmatrix} : t \in \mathbb{R} \right\}.$$

Similarly, for  $f_0(x, y) = x^2 - y^2$ , the group  $O_{f_0}(\mathbb{R})$  is the usual split orthogonal group

$$(4.13) \quad \begin{aligned} O(1, 1) = & \left\{ \pm \begin{pmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{pmatrix} : t \in \mathbb{R} \right\} \cup \left\{ \pm \begin{pmatrix} \sinh t & \cosh t \\ -\cosh t & -\sinh t \end{pmatrix} : t \in \mathbb{R} \right\} \\ & \cup \left\{ \pm \begin{pmatrix} \sinh t & \cosh t \\ \cosh t & \sinh t \end{pmatrix} : t \in \mathbb{R} \right\} \cup \left\{ \pm \begin{pmatrix} \cosh t & \sinh t \\ -\sinh t & -\cosh t \end{pmatrix} : t \in \mathbb{R} \right\}. \end{aligned}$$

Recall the notation in Section 4.2 and that  $\delta^{-1/2} \cdot f = (f_0)_{T_f}$ , where  $\delta = D/4$  and  $D$  is the absolute value of the discriminant of  $f$ . Then, we have

$$(4.14) \quad O_f(\mathbb{R}) = T_f^{-1}(O_{f_0}(\mathbb{R}))T_f.$$

We then see that if  $f$  is positive definite, then elements in  $O_f(\mathbb{R})$  are of the forms

$$(4.15) \quad \begin{pmatrix} \phi_t + \frac{\beta\psi_t}{2\sqrt{\delta}} & \frac{\gamma\psi_t}{\sqrt{\delta}} \\ -\frac{\alpha\psi_t}{\sqrt{\delta}} & \phi_t - \frac{\beta\psi_t}{2\sqrt{\delta}} \end{pmatrix} \text{ and } \begin{pmatrix} \phi_t - \frac{\beta\psi_t}{2\sqrt{\delta}} & \frac{\beta}{\alpha} \left( \phi_t - \frac{\beta\psi_t}{2\sqrt{\delta}} \right) + \frac{\gamma\psi_t}{\sqrt{\delta}} \\ \frac{\alpha\psi_t}{\sqrt{\delta}} & -\phi_t - \frac{\beta\psi_t}{2\sqrt{\delta}} \end{pmatrix},$$

where  $t \in \mathbb{R}$  and  $(\phi_t, \psi_t) = (\cos t, \sin t)$ . If  $f$  is indefinite, then up to sign, elements in  $O_f(\mathbb{R})$  are of the forms

$$(4.16) \quad \begin{pmatrix} \phi_t - \frac{\beta\psi_t}{2\sqrt{\delta}} & -\frac{\gamma\psi_t}{\sqrt{\delta}} \\ \frac{\alpha\psi_t}{\sqrt{\delta}} & \phi_t + \frac{\beta\psi_t}{2\sqrt{\delta}} \end{pmatrix} \text{ and } \begin{pmatrix} \phi_t + \frac{\beta\psi_t}{2\sqrt{\delta}} & \frac{\beta}{\alpha} \left( \phi_t + \frac{\beta\psi_t}{2\sqrt{\delta}} \right) - \frac{\gamma\psi_t}{\sqrt{\delta}} \\ -\frac{\alpha\psi_t}{\sqrt{\delta}} & -\phi_t - \frac{\beta\psi_t}{2\sqrt{\delta}} \end{pmatrix},$$

where  $t \in \mathbb{R}$  and  $(\phi_t, \psi_t) \in \{(\cosh t, \sinh t), (\sinh t, \cosh t)\}$ . We note that the matrices in (4.16) are obtained by conjugating  $\begin{pmatrix} \phi_t & \psi_t \\ \psi_t & \phi_t \end{pmatrix}$  and  $\begin{pmatrix} \phi_t & \psi_t \\ -\psi_t & -\phi_t \end{pmatrix}$ , respectively, by  $T_f$ .

First, we shall determine when  $O_f(\mathbb{Z})$  contains a non-trivial torsion element. It will be helpful to recall Definition 1.1.

**Lemma 4.10.** *If  $O_f(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}$  contains a matrix  $T$  of finite order, then  $f$  is either reducible, ambiguous, or opaque. And if  $T$  may be taken to have negative determinant, then  $f$  is either reducible or ambiguous.*

*Proof.* Up to  $\text{GL}_2(\mathbb{Z})$ -conjugation, there are five cyclic subgroups of  $\text{GL}_2(\mathbb{Z})$  not contained in  $\{\pm I_{2 \times 2}\}$  (see [11, p. 180], for example), and they may be taken to be

$$\left\langle \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

So, there exists  $P \in \text{GL}_2(\mathbb{Z})$  such that up to sign, the matrix  $Q = P^{-1}TP$  is equal to

$$Q_1 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, Q_2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, Q_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, Q_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Q_5 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Note that  $\det(Q_i) = 1$  for  $i = 1, 2, 3$  and  $\det(Q_i) = -1$  for  $i = 4, 5$ . Since  $Q \in O_{f_P}(\mathbb{Z})$ , writing  $f_P(x, y) = ax^2 + bxy + cy^2$ , we then see that

$$\begin{cases} a = -b \text{ or } c = 0 & \text{if } Q = \pm Q_1 \\ a = -b \text{ or } a = 0 & \text{if } Q = \pm Q_2 \\ a = -c \text{ or } b = 0 & \text{if } Q = \pm Q_3 \end{cases} \text{ and } \begin{cases} a = 0 \text{ or } b = 0 & \text{if } Q = \pm Q_4 \\ a = c \text{ or } b = 0 & \text{if } Q = \pm Q_5. \end{cases}$$

This shows that  $f$  is ambiguous, reducible, or  $\text{GL}_2(\mathbb{Z})$ -equivalent to  $ax^2 + bxy \pm ay^2$ . Since  $ax^2 + bxy + ay^2$  is ambiguous via the matrix  $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ , the claim now follows.  $\square$

**Proposition 4.11.** *Assume that  $f$  is primitive, positive definite, and reduced. Then*

$$O_f(\mathbb{Z}) = \begin{cases} \{\pm I_{2 \times 2}\} & \text{if } f \text{ is not ambiguous} \\ \{\pm I_{2 \times 2}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\} & \text{if } f(x, y) = x^2 + y^2 \\ \{\pm I_{2 \times 2}, \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\} & \text{if } f(x, y) = \alpha x^2 + \gamma y^2, \alpha < \gamma \\ \{\pm I_{2 \times 2}, \pm \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \\ \quad \pm \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}\} & \text{if } f(x, y) = x^2 + xy + y^2 \\ \{\pm I_{2 \times 2}, \pm \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\} & \text{if } f(x, y) = \alpha x^2 + \alpha xy + \gamma y^2, \alpha < \gamma. \end{cases}$$

*Proof.* Elements in  $O_f(\mathbb{Z})$  have finite orders by (4.12) and (4.14). Hence, if  $f$  is not ambiguous, then  $O_f(\mathbb{Z}) = \{\pm I_{2 \times 2}\}$  by Lemma 4.10. It is known to Gauss [10] that every ambiguous form is  $\text{GL}_2(\mathbb{Z})$ -equivalent to a reduced form of the shape  $ax^2 + bxy + cy^2$  with  $a$  dividing  $b$ . Since every positive definite form is  $\text{GL}_2(\mathbb{Z})$ -equivalent to a unique reduced form, if  $f$  is ambiguous, then  $\alpha$  divides  $\beta$ , and so  $\beta \in \{0, \alpha\}$  by Definition 1.1.

Now, consider  $T \in O_f(\mathbb{Z})$ , which is equal to one of the matrices in (4.15) for some  $t \in \mathbb{R}$ . If  $\beta = 0$ , then  $|\cos t| \in \{0, 1\}$ , and also  $\alpha \sin t / \sqrt{\alpha\gamma}, \gamma \sin t / \sqrt{\alpha\gamma} \in \mathbb{Z}$ . Since  $\alpha$  and  $\gamma$  are coprime, we have  $\cos t = 0$ , that is  $|\sin t| = 1$ , only if  $\alpha = \gamma = 1$ . We easily see from here that  $O_f(\mathbb{Z})$  is as stated. If  $\alpha = \beta$ , then  $T$  is of the form

$$\begin{pmatrix} \cos t + \frac{\alpha \sin t}{\sqrt{D}} & \frac{2\gamma \sin t}{\sqrt{D}} \\ -\frac{2\alpha \sin t}{\sqrt{D}} & \cos t - \frac{\alpha \sin t}{\sqrt{D}} \end{pmatrix} \text{ or } \begin{pmatrix} \cos t - \frac{\alpha \sin t}{\sqrt{D}} & \cos t + \frac{(2\gamma - \alpha) \sin t}{\sqrt{D}} \\ \frac{2\alpha \sin t}{\sqrt{D}} & -\cos t + \frac{\alpha \sin t}{\sqrt{D}} \end{pmatrix},$$

where  $D = \alpha(4\gamma - \alpha)$ . It is easy to see that  $D \neq 1, 4$ . Also, we must have

$$2 \cos t, (2\alpha \sin t)/\sqrt{D}, (2\gamma \sin t)/\sqrt{D} \in \mathbb{Z}.$$

Since  $\alpha$  and  $\gamma$  are coprime, we then see that  $|\sin t| \neq 1$  and that  $|\sin t| = \sqrt{3}/2$  only if  $D = 3$ . Hence, we have  $|\cos t| \in \{1/2, 1\}$ , and  $|\cos t| = 1/2$  only if  $D = 3$ , in which case  $\alpha = \gamma = 1$ . From here, it is easy to check that  $O_f(\mathbb{Z})$  is as stated.  $\square$

**Proposition 4.12.** *Assume that  $f$  is primitive, reducible, and reduced. We have*

$$O_f(\mathbb{Z}) = \begin{cases} \{\pm I_{2 \times 2}\} & \text{if } \beta \nmid \alpha^2 + 1 \text{ and } \beta \nmid \alpha^2 - 1 \\ \left\{ \pm I_{2 \times 2}, \pm \begin{pmatrix} \alpha & \beta \\ -\frac{\alpha^2+1}{\beta} & -\alpha \end{pmatrix} \right\} & \text{if } \beta \mid \alpha^2 + 1 \text{ and } \beta \nmid \alpha^2 - 1 \\ \left\{ \pm I_{2 \times 2}, \pm \begin{pmatrix} \alpha & \beta \\ -\frac{\alpha^2-1}{\beta} & -\alpha \end{pmatrix} \right\} & \text{if } \beta \nmid \alpha^2 + 1 \text{ and } \beta \mid \alpha^2 - 1 \\ \{\pm I_{2 \times 2}, \pm \begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ -2 & -1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\} & \text{if } f(x, y) = x^2 + xy \\ \{\pm I_{2 \times 2}, \pm \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}\} & \text{if } f(x, y) = x^2 + 2xy. \end{cases}$$

*Proof.* Note that  $\gamma = 0$  and  $\beta > 0$  by Definition 1.1. Consider  $T \in O_f(\mathbb{Z})$ . By (4.16), we know that  $\pm T$  is equal to

$$\begin{pmatrix} \phi_t - \psi_t & 0 \\ \frac{2\alpha\psi_t}{\beta} & \phi_t + \psi_t \end{pmatrix} \text{ or } \begin{pmatrix} \phi_t + \psi_t & \frac{\beta}{\alpha}(\phi_t + \psi_t) \\ -\frac{2\alpha\psi_t}{\beta} & -\phi_t - \psi_t \end{pmatrix},$$

where  $(\phi_t, \psi_t) \in \{(\cosh t, \sinh t), (\sinh t, \cosh t)\}$  and  $t \in \mathbb{R}$ .

If  $\pm T$  is equal to the matrix on the left, then  $2 \cosh t, 2 \sinh t \in \mathbb{Z}$ . Since

$$(2 \cosh t + 2 \sinh t)(2 \cosh t - 2 \sinh t) = 4,$$

we must have  $(2 \cosh t, 2 \sinh t) = (2, 0)$ . It follows that  $\pm T = I_{2 \times 2}$  or  $\pm T = \begin{pmatrix} -1 & 0 \\ 2\alpha/\beta & 1 \end{pmatrix}$ . Since  $\alpha$  and  $\beta$  are coprime, in the latter case  $\beta$  divides 2 and so  $f(x, y) = x^2 + \beta xy$ . If  $\pm T$  is equal to the matrix on the right, then  $2\alpha \cosh t, 2\alpha \sinh t \in \mathbb{Z}$ . We must also have  $\cosh t + \sinh t \in \alpha\mathbb{Z}$  since  $\alpha$  and  $\beta$  are coprime. Since

$$(\cosh t + \sinh t)(2\alpha \cosh t - 2\alpha \sinh t) = 2\alpha,$$

we find that  $(2\alpha \cosh t, 2\alpha \sinh t) = (\alpha^2 + 1, \alpha^2 - 1)$ , and thus  $\pm T = \begin{pmatrix} \alpha & \beta \\ -(\alpha^2 \pm 1)/\beta & -\alpha \end{pmatrix}$ . Putting everything together, we see that  $O_f(\mathbb{Z})$  is as stated.  $\square$

Finally, we address the case when  $f$  is irreducible and indefinite. For  $D \in \mathbb{N}$  which is not a square, recall the notation preceding Theorem 1.4 and define

$$(4.17) \quad T_D = \begin{pmatrix} \frac{u_D - \beta v_D}{2} & -\gamma v_D \\ \alpha v_D & \frac{u_D + \beta v_D}{2} \end{pmatrix}.$$

Notice that  $T_D \in \text{GL}_2(\mathbb{Z})$ , and write  $G_f(\mathbb{Z})$  for the subgroup of  $\text{GL}_2(\mathbb{Z})$  consisting of the matrices  $\pm T_D^n$  for  $n \in \mathbb{Z}$ . Elements in  $G_f(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}$  have infinite orders.

**Proposition 4.13.** *Assume that  $f$  is primitive, indefinite, and irreducible. Write  $D$  for the discriminant of  $f$ . We have*

$$O_f(\mathbb{Z}) = \begin{cases} G_f(\mathbb{Z}) & \text{if } f \text{ is neither ambiguous nor opaque} \\ G_f(\mathbb{Z}) \sqcup \begin{pmatrix} 1 & \beta/\alpha \\ 0 & -1 \end{pmatrix} G_f(\mathbb{Z}) & \text{if } f \text{ is ambiguous, and we assume } \alpha \text{ divides } \beta \\ G_f(\mathbb{Z}) \sqcup \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} G_f(\mathbb{Z}) & \text{if } f \text{ is opaque, and we assume } \alpha = -\gamma. \end{cases}$$

Moreover, the set of matrices in  $O_f(\mathbb{Z})$  of infinite orders is precisely  $G_f(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}$ .

*Proof.* By (4.13) and (4.16), elements in  $O_f(\mathbb{R})$  having infinite order are precisely the matrices other than  $\pm I_{2 \times 2}$  of the shape

$$\pm \begin{pmatrix} \frac{x - \beta y}{2} & -\gamma y \\ \alpha y & \frac{x + \beta y}{2} \end{pmatrix}, \text{ where } x^2 - Dy^2 = \pm 4.$$

Since  $\alpha, \beta$ , and  $\gamma$  are coprime, the above has integer entries if and only if  $(x, y) \in \mathbb{Z}^2$ . By the minimality of  $(u_D, v_D)$ , it follows that the set of matrices in  $O_f(\mathbb{Z})$  of infinite order is precisely  $G_f(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}$ .

If  $f$  is not ambiguous nor opaque, then  $O_f(\mathbb{Z})$  has no element of finite order other than  $\pm I_{2 \times 2}$  by Lemma 4.10, and we are done. So, suppose that  $\alpha$  divides  $\beta$  or  $\alpha = -\gamma$ .

First, note that by (4.13) and (4.14), elements in  $O_f(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}$  of finite order must be of the shape  $\pm T_f^{-1} T T_f$ , where

$$(4.18) \quad T \in \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \sinh t & \cosh t \\ -\cosh t & -\sinh t \end{pmatrix}, \begin{pmatrix} \cosh t & \sinh t \\ -\sinh t & -\cosh t \end{pmatrix} \right\}$$

where  $t \in \mathbb{R}$ . But by (4.16), we have

$$(4.19) \quad T_f^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} T_f = \begin{pmatrix} -\frac{\beta}{\sqrt{D}} & -\frac{2\gamma}{\sqrt{D}} \\ \frac{2\alpha}{\sqrt{D}} & \frac{\beta}{\sqrt{D}} \end{pmatrix},$$

which cannot have integer coefficients since  $D$  is not a square. Using this and (4.14), we then check that if  $M, M' \in O_f(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}$  both have finite orders and  $M' \neq \pm M$ , then  $MM' \in O_f(\mathbb{Z})$  has infinite order. Take

$$(4.20) \quad M = \begin{cases} \begin{pmatrix} 1 & \beta/\alpha \\ 0 & -1 \end{pmatrix} & \text{if } \alpha \text{ divides } \beta \\ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \text{if } \alpha = -\gamma, \end{cases}$$

which is an element in  $O_f(\mathbb{Z})$  of orders 2 and 4, respectively. It follows that elements in  $O_f(\mathbb{Z}) \setminus \{\pm I_{2 \times 2}\}$  of finite order are precisely the matrices in  $MG_f(\mathbb{Z})$ , and the claim now follows.  $\square$

**4.4. Proof of Theorem 1.5.** If  $x^2 - Dy^2 = -4$  is soluble in integers  $x$  and  $y$ , then take  $f(x, y) = ax^2 + bxy - ay^2$ , which is primitive and opaque of discriminant  $D$ . Note that  $T_D \in G_f(\mathbb{Z})$  has negative determinant because  $D$  is of negative type. Proposition 4.13 then implies that  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} T_D \in O_f(\mathbb{Z})$ , which has negative determinant and finite order, whence  $f$  is also ambiguous by Lemma 4.10.

Conversely, if there exists a primitive, integral, ambiguous, and opaque binary quadratic form  $f$  of discriminant  $D$ , then the third case of Proposition 4.13 implies that  $O_f(\mathbb{Z})$  contains an element of positive determinant and finite order. The second case of Proposition 4.13 in turn shows that  $G_f(\mathbb{Z})$  must have an element of negative determinant. This means that  $T_D \in G_f(\mathbb{Z})$  has negative determinant and so  $x^2 - Dy^2 = -4$  is soluble in integers  $x$  and  $y$ .

## 5. PARAMETRIZING FORMS IN $V_{\mathbb{R},f}$ OF NON-ZERO DISCRIMINANTS

Our aim in this section is to parametrize elements in  $V_{\mathbb{R},f}^0$  with the following data: values of the  $L_f$ - and  $K_f$ -invariants defined in Section 3.1, and elements in  $O_f(\mathbb{R})$  of determinant one. In view of (4.10), it will suffice to consider the form  $f_0(x, y)$  defined as in (4.8). The case when  $f$  is reducible will be treated separately because then we identify  $V_{\mathbb{R},f}$  with  $\mathbb{R}^3$  via (3.5) rather than (3.2).

In view of (1.4), define

$$(5.1) \quad \begin{aligned} \Omega^0 &= \{(L, K) \in \mathbb{R}^2 \mid L^2 + 4K \neq 0 \text{ and } 2L^2 - K \neq 0\} \\ \Omega^+ &= \{(L, K) \in \mathbb{R}^2 \mid L^2 + 4K > 0 \text{ and } 2L^2 - K \neq 0\} \\ \Omega^- &= \{(L, K) \in \mathbb{R}^2 \mid L^2 + 4K < 0 \text{ and } 2L^2 - K \neq 0\}. \end{aligned}$$

Note that for any  $F \in V_{\mathbb{R},f}^0$ , we have  $(L_f(F), K_f(F)) \in \Omega^0$ . Also, we have  $\Delta(F) > 0$  if and only if  $(L_f(F), K_f(F)) \in \Omega^+$ , and  $\Delta(F) < 0$  if and only if  $(L_f(F), K_f(F)) \in \Omega^-$ .



**5.1. Positive definite case.** Consider the case  $f_0(x, y) = x^2 + y^2$ . Recall from (3.1) that an element in  $V_{\mathbb{R}, f_0}$  is of the form

$$(5.2) \quad F(x, y) = a_4x^4 + a_3x^3y + a_2x^2y^2 - a_3xy^3 + a_4y^4.$$

A simple calculation shows that

$$(5.3) \quad \Delta(F) = (4a_4(2a_4 + a_2) - a_3^2)^2((2a_4 - a_2)^2 + 4a_3^2).$$

Note that  $\Delta(F) \geq 0$ . Also, recall (4.12), and for each  $t \in \mathbb{R}$  put

$$T^+(t) = \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}.$$

Note that by Lemmas 4.6 and 4.7, we have  $F_{T^+(t)} \in V_{\mathbb{R}, f_0}^0$  for all  $F \in V_{\mathbb{R}, f_0}^0$ .

**Lemma 5.1.** *Let  $F \in V_{\mathbb{R}, f_0}^0$  be as in (5.2) and let  $t \in \mathbb{R}$ . Then, we have*

$$F_{T^+(t)}(x, y) = A(t)x^4 + B(t)x^3y + C(t)x^2y^2 - B(t)xy^3 + A(t)y^4,$$

where

$$(5.4) \quad \begin{cases} A(t) = \frac{6a_4 + a_2}{8} + \frac{2a_4 - a_2}{8} \cos(4t) - \frac{a_3}{4} \sin(4t) \\ B(t) = a_3 \cos(4t) + \frac{2a_4 - a_2}{2} \sin(4t) \\ C(t) = \frac{6a_4 + a_2}{4} - \frac{3(2a_4 - a_2)}{4} \cos(4t) + \frac{3a_3}{2} \sin(4t). \end{cases}$$

Moreover, there exists a unique  $t \in (-\pi/4, \pi/4]$  with  $B(t) = 0$  and  $2A(t) - C(t) > 0$ .

*Proof.* The formulae in (5.4) follow from a straightforward computation. The conditions  $B(t) = 0$  and  $2A(t) - C(t) > 0$  are equivalent to

$$(5.5) \quad \begin{cases} (2a_4 - a_2) \sin(4t) + 2a_3 \cos(4t) = 0 \\ (2a_4 - a_2) \cos(4t) - 2a_3 \sin(4t) > 0. \end{cases}$$

Note that  $2a_4 - a_2 = 0$  and  $a_3 = 0$  cannot occur simultaneously by (5.3). We then see that the equation in (5.5) has exactly two solutions  $4t \in (-\pi, \pi]$  of the forms  $4t = 4t_0$  and  $4t = 4t_0 - \pi$ , where  $4t_0 \in (0, \pi]$ . Observe that

$$(2a_4 - a_2) \cos(4t_0 - \pi) - 2a_3 \sin(4t_0 - \pi) = -((2a_4 - a_2) \cos(4t_0) - 2a_3 \sin(4t_0)).$$

Hence, exactly one of  $t = t_0$  and  $t = t_0 - \pi/4$  satisfies the inequality in (5.5). Thus, indeed (5.5) has a unique solution  $t \in (-\pi/4, \pi/4]$ , as desired.  $\square$

Lemma 5.1 has the following consequence.

**Lemma 5.2.** *Let  $F \in V_{\mathbb{R}, f_0}^0$  be given, and write  $L = L_{f_0}(F)$  and  $K = K_{f_0}(F)$ . Then, we have  $L^2 + 4K > 0$ , and there exists a unique  $t \in [-\pi/4, \pi/4)$  such that*

$$F(x, y) = (F_{(L, K)})_{T^+(t)}(x, y),$$

where

$$F_{(L, K)}(x, y) = \frac{-3L + \sqrt{L^2 + 4K}}{24}x^4 + \frac{-L - \sqrt{L^2 + 4K}}{4}x^2y^2 + \frac{-3L + \sqrt{L^2 + 4K}}{24}y^4.$$

*Proof.* We have  $\Delta(F) > 0$  by (5.3) and hence  $L^2 + 4K > 0$  by (1.4). Now, uniqueness is clear from Lemma 5.1. To show existence, again by Lemma 5.1, we know that there exists  $-t \in (-\pi/4, \pi/4]$  such that  $F_{T+(-t)}(x, y)$  is of the form

$$Ax^4 + Cx^2y^2 + Ay^4$$

with  $2A - C > 0$ . Using Propositions 3.4 and 3.6, we compute that

$$L = -6A - C \text{ and } K = -2C(6A - C).$$

The above system, together with the inequality  $2A - C > 0$ , we see that has exactly one solution given by

$$(A, C) = \left( \frac{-3L + \sqrt{L^2 + 4K}}{24}, \frac{-L - \sqrt{L^2 + 4K}}{4} \right).$$

Thus, we have  $F_{T+(-t)}(x, y) = F_{(L,K)}(x, y)$ , as claimed.  $\square$

Recall (5.1), and note that Lemma 5.2 implies that we have a map

$$\Phi : \Omega^+ \times [-\pi/4, \pi/4] \rightarrow V_{\mathbb{R}, f_0}^0; \quad \Phi(L, K, t) = (F_{(L,K)})_{T+(t)}.$$

Identifying  $V_{\mathbb{R}, f_0}$  with  $\mathbb{R}^3$  via (3.2), we deduce from (5.4) that

$$\Phi(L, K, t) = (\Phi_1(L, K, t), \Phi_2(L, K, t), \Phi_3(L, K, t)),$$

where

$$(5.6) \quad \begin{cases} \Phi_1(L, K, t) = -\frac{L}{8} + \frac{\sqrt{L^2 + 4K}}{24} \cos(4t) \\ \Phi_2(L, K, t) = \frac{\sqrt{L^2 + 4K}}{6} \sin(4t) \\ \Phi_3(L, K, t) = -\frac{L}{4} - \frac{\sqrt{L^2 + 4K}}{4} \cos(4t). \end{cases}$$

Notice that by Proposition 3.4, the form  $\Phi(L, K, t)$  has  $L_{f_0}$ - and  $K_{f_0}$ -invariants equal to  $L$  and  $K$ , respectively.

**Proposition 5.3.** *The map  $\Phi$  is a bijection and its Jacobian*

$$\mathfrak{J} = \begin{pmatrix} \frac{\partial \Phi_1}{\partial L} & \frac{\partial \Phi_1}{\partial K} & \frac{\partial \Phi_1}{\partial t} \\ \frac{\partial \Phi_2}{\partial L} & \frac{\partial \Phi_2}{\partial K} & \frac{\partial \Phi_2}{\partial t} \\ \frac{\partial \Phi_3}{\partial L} & \frac{\partial \Phi_3}{\partial K} & \frac{\partial \Phi_3}{\partial t} \end{pmatrix}$$

*has determinant equal to  $-1/18$ .*

*Proof.* That  $\Phi$  is a bijection follows from Lemma 5.2 and that  $\det(\mathfrak{J}) = -1/18$  follows from a direct computation.  $\square$

**5.2. Indefinite case.** Consider the case  $f_0(x, y) = x^2 - y^2$ . Recall from (3.1) that an element in  $V_{\mathbb{R}, f_0}$  is of the form

$$(5.7) \quad F(x, y) = a_4x^4 + a_3x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4.$$

A simple calculation shows that

$$(5.8) \quad \Delta(F) = (2a_4 - 2a_3 + a_2)(2a_4 + 2a_3 + a_2)(8a_4^2 - 4a_4a_2 + a_3^2)^2.$$

Next, recall (4.13), and for each  $t \in \mathbb{R}$  put

$$(5.9) \quad T^-(t) = \begin{pmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{pmatrix}.$$

Notice that by Lemmas 4.6 and 4.7, we have  $F_{T^-(t)} \in V_{\mathbb{R}, f_0}^0$  for all  $F \in V_{\mathbb{R}, f_0}^0$ . Then, analogously to Lemma 5.1, we have the following.

**Lemma 5.4.** *Let  $F \in V_{\mathbb{R}, f_0}^0$  be as in (5.7) and let  $t \in \mathbb{R}$ . Then, we have*

$$F_{T^-(t)}(x, y) = A(t)x^4 + B(t)x^3y + C(t)x^2y^2 + B(t)xy^3 + A(t)y^4,$$

where

$$(5.10) \quad \begin{cases} A(t) = \frac{6a_4 - a_2}{8} + \frac{2a_4 + a_2}{8} \cosh(4t) + \frac{a_3}{4} \sinh(4t) \\ B(t) = a_3 \cosh(4t) + \frac{2a_4 + a_2}{2} \sinh(4t) \\ C(t) = -\frac{6a_4 - a_2}{4} + \frac{3(2a_4 + a_2)}{4} \cosh(4t) + \frac{3a_3}{2} \sinh(4t). \end{cases}$$

If  $\Delta(F) > 0$ , then there exists a unique  $t \in \mathbb{R}$  such that  $B(t) = 0$ . If  $\Delta(F) < 0$ , then we have  $B(t) \neq 0$  for all  $t \in \mathbb{R}$  and there exists a unique  $t \in \mathbb{R}$  such that  $A(t) = 0$ .

*Proof.* The formulae in (5.10) follows from a direct computation. Next, we rewrite

$$A(t) = \frac{6a_4 - a_2}{8} + \left( \frac{2a_4 + 2a_3 + a_2}{16} \right) e^{4t} + \left( \frac{2a_4 - 2a_3 + a_2}{16} \right) e^{-4t}$$

and similarly

$$B(t) = \left( \frac{2a_4 + 2a_3 + a_2}{4} \right) e^{4t} - \left( \frac{2a_4 - 2a_3 + a_2}{4} \right) e^{-4t}.$$

Then, the equation  $B(t) = 0$  is equivalent to

$$(5.11) \quad (2a_4 + 2a_3 + a_2)e^{8t} - (2a_4 - 2a_3 + a_2) = 0.$$

Note that  $2a_4 + 2a_3 + a_2, 2a_4 - 2a_3 + a_2 \neq 0$  by (5.8). If  $\Delta(F) > 0$ , then  $2a_4 + 2a_3 + a_2$  and  $2a_4 - 2a_3 + a_2$  have the same sign, and hence (5.11) has a unique solution  $t \in \mathbb{R}$ . Analogously, if  $\Delta(F) < 0$ , then  $2a_4 + 2a_3 + a_2$  and  $2a_4 - 2a_3 + a_2$  have opposite signs, and hence (5.11) has no solution in  $\mathbb{R}$ . Since  $\frac{d}{dt}A(t) = \frac{1}{2}B(t)$ , as a map from  $\mathbb{R}$  to  $\mathbb{R}$ , we see that  $A(t)$  is strictly monotone in this case. Since  $2a_4 + 2a_3 + a_2, 2a_4 - 2a_3 + a_2 \neq 0$ , the map  $A(t)$  does not possess any horizontal asymptotes and hence is a bijection. It follows that  $A(t) = 0$  for a unique  $t \in \mathbb{R}$ .  $\square$

We now obtain the following analogue of Lemma 5.2.

**Lemma 5.5.** *Let  $F \in V_{\mathbb{R}, f_0}^0$  be given, and write  $L = L_{f_0}(F)$  and  $K = K_{f_0}(F)$ .*

(a) If  $\Delta(F) > 0$ , then  $L^2 + 4K > 0$  and there exists a unique pair  $(t, i) \in \mathbb{R} \times \{1, 2\}$  such that

$$F(x, y) = (F_{(L,K)}^{(i)})_{T-(t)}(x, y),$$

where

$$F_{(L,K)}^{(i)}(x, y) = \frac{3L + (-1)^i \sqrt{L^2 + 4K}}{24} x^4 + \frac{-L + (-1)^i \sqrt{L^2 + 4K}}{4} x^2 y^2 + \frac{3L + (-1)^i \sqrt{L^2 + 4K}}{24} y^4.$$

(b) If  $\Delta(F) < 0$ , then  $2L^2 - K > 0$  and there exists a unique pair  $(t, i) \in \mathbb{R} \times \{3, 4\}$  such that

$$F(x, y) = (F_{(L,K)}^{(i)})_{T-(t)}(x, y),$$

where

$$F_{(L,K)}^{(i)}(x, y) = \frac{(-1)^i \sqrt{2L^2 - K}}{3} x^3 y - L x^2 y^2 + \frac{(-1)^i \sqrt{2L^2 - K}}{3} x y^3.$$

*Proof.* First, suppose that  $\Delta(F) > 0$ , in which case  $L^2 + 4K > 0$  by (1.4). Uniqueness is clear from Lemma 5.4. As for existence, again by Lemma 5.4, we know that there exists  $-t \in \mathbb{R}$  such that  $F_{T-(-t)}(x, y)$  is of the form

$$Ax^4 + Cx^2y^2 + Ay^4.$$

Using Propositions 3.4 and 3.6, we compute that

$$L = 6A - C \text{ and } K = 2C(6A + C).$$

The above system has exactly two solutions, namely

$$(A, C) = \left( \frac{3L + (-1)^i \sqrt{L^2 + 4K}}{24}, \frac{-L + (-1)^i \sqrt{L^2 + 4K}}{4} \right)$$

for  $i \in \{1, 2\}$ . It follows that  $F_{T-(-t)}(x, y) = F_{(L,K)}^{(i)}(x, y)$  for  $i \in \{1, 2\}$ , as desired.

Next, suppose that  $\Delta(F) < 0$ , in which case  $L^2 + 4K < 0$  by (1.4). So then  $K < 0$  and  $2L^2 - K > 0$  holds. Uniqueness is clear from Lemma 5.4. As for existence, again by Lemma 5.4, there exists  $t \in \mathbb{R}$  such that  $F_{T^{-1}(t)}(x, y)$  is of the form

$$Bx^3y + Cx^2y^2 + Bxy^3.$$

Using Propositions 3.4 and 3.6, we compute that

$$L = -C \text{ and } K = -9B^2 + 2C^2.$$

The above system has exactly two solutions, namely

$$(B, C) = \left( \frac{(-1)^i \sqrt{2L^2 - K}}{3}, -L \right)$$

for  $i \in \{3, 4\}$ . It follows that  $F_{T-(-t)}(x, y) = F_{(L,K)}^{(i)}(x, y)$  for  $i \in \{3, 4\}$ , as desired.  $\square$

Now, recall (5.1), and further define

$$V_{\mathbb{R},f_0}^{0,+} = \{F \in V_{\mathbb{R},f_0}^0 \mid \Delta(F) > 0\} \text{ and } V_{\mathbb{R},f_0}^{0,-} = \{F \in V_{\mathbb{R},f_0}^0 \mid \Delta(F) < 0\}.$$

Then, Lemma 5.5 (a) implies that for  $i = 1, 2$ , we have a map

$$\Phi^{(i)} : \Omega^+ \times \mathbb{R} \longrightarrow V_{\mathbb{R},f_0}^{0,+}; \quad \Phi^{(i)}(L, K, t) = (F_{(L,K)}^{(i)})_{T^-(t)}.$$

Identifying  $V_{\mathbb{R},f_0}$  with  $\mathbb{R}^3$  via (3.2), we deduce from (5.10) that

$$\Phi^{(i)}(L, K, t) = (\Phi_1^{(i)}(L, K, t), \Phi_2^{(i)}(L, K, t), \Phi_3^{(i)}(L, K, t)),$$

where

$$(5.12) \quad \begin{cases} \Phi_1^{(i)}(L, K, t) = \frac{L}{8} + \frac{(-1)^i \sqrt{L^2 + 4K}}{24} \cosh(4t), \\ \Phi_2^{(i)}(L, K, t) = \frac{(-1)^i \sqrt{L^2 + 4K}}{6} \sinh(4t) \\ \Phi_3^{(i)}(L, K, t) = -\frac{L}{4} + \frac{(-1)^i \sqrt{L^2 + 4K}}{4} \cosh(4t). \end{cases}$$

Similarly, by Lemma 5.5 (b), for  $i = 3, 4$ , we have a map

$$\Phi^{(i)} : \Omega^- \times \mathbb{R} \longrightarrow V_{\mathbb{R},f_0}^{0,-}; \quad \Phi^{(i)}(L, K, t) = (F_{(L,K)}^{(i)})_{T^-(t)}.$$

Identifying  $V_{\mathbb{R},f_0}$  with  $\mathbb{R}^3$  via (3.2), we deduce from (5.10) that

$$\Phi^{(i)}(L, K, t) = (\Phi_1^{(i)}(L, K, t), \Phi_2^{(i)}(L, K, t), \Phi_3^{(i)}(L, K, t)),$$

where

$$(5.13) \quad \begin{cases} \Phi_1^{(i)}(L, K, t) = \frac{L}{8} - \frac{L}{8} \cosh(4t) + \frac{(-1)^i \sqrt{2L^2 - K}}{12} \sinh(4t) \\ \Phi_2^{(i)}(L, K, t) = \frac{(-1)^i \sqrt{2L^2 - K}}{3} \cosh(4t) - \frac{L}{2} \sinh(4t) \\ \Phi_3^{(i)}(L, K, t) = -\frac{L}{4} - \frac{3L}{4} \cosh(4t) + \frac{(-1)^i \sqrt{2L^2 - K}}{2} \sinh(4t). \end{cases}$$

Note that by Proposition 3.4, the form  $\Phi^{(i)}(L, K, t)$  has  $L_{f_0}$ - and  $K_{f_0}$ -invariants equal to  $L$  and  $K$ , respectively, for all  $i = 1, 2, 3, 4$ .

**Proposition 5.6.** *For all  $i = 1, 2, 3, 4$ , the map  $\Phi^{(i)}$  is an injection and its Jacobian*

$$\mathfrak{J}^{(i)} = \begin{pmatrix} \frac{\partial \Phi_1^{(i)}}{\partial L} & \frac{\partial \Phi_1^{(i)}}{\partial K} & \frac{\partial \Phi_1^{(i)}}{\partial t} \\ \frac{\partial \Phi_2^{(i)}}{\partial L} & \frac{\partial \Phi_2^{(i)}}{\partial K} & \frac{\partial \Phi_2^{(i)}}{\partial t} \\ \frac{\partial \Phi_3^{(i)}}{\partial L} & \frac{\partial \Phi_3^{(i)}}{\partial K} & \frac{\partial \Phi_3^{(i)}}{\partial t} \end{pmatrix}$$

has determinant equal to  $-1/18$ . Moreover, we have

$$(5.14) \quad V_{\mathbb{R},f_0}^{0,+} = \bigsqcup_{i=1}^2 \Phi^{(i)}(\Omega^+ \times \mathbb{R}) \text{ and } V_{\mathbb{R},f_0}^{0,-} = \bigsqcup_{i=3}^4 \Phi^{(i)}(\Omega^- \times \mathbb{R}).$$

*Proof.* That  $\Phi^{(i)}$  is an injection and that (5.14) holds follow from Lemma 5.5. As for the claim that  $\det(\mathfrak{J}^{(i)}) = -1/18$ , it may be verified by explicit computation.  $\square$

In Lemma 5.4, we considered the action of  $T^-(t)$  on  $V_{\mathbb{R},f_0}^0$ . Recall from (4.13) that elements in  $O(1,1)$  are of the forms  $\pm J_k T^-(t)$  for  $k = 1, 2, 3, 4$ , where  $t \in \mathbb{R}$  and

$$(5.15) \quad J_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, J_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, J_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The lemma below describes the action of  $J_k$  for  $k = 1, 2, 3, 4$ , and therefore the action of  $O(1,1)$ , on the forms in  $V_{\mathbb{R},f}^0$ . This will be needed in the proof of Theorem 1.4 (a) in order to determine the value of  $r_f$  defined in (4.2).

**Lemma 5.7.** *Let  $F \in V_{\mathbb{R},f}^0$  be given, and write*

$$F = (F_{(L,K)}^{(i)})_{T^-(t)},$$

*where  $L = L_{f_0}(F)$ ,  $K = K_{f_0}(F)$ , and  $(t, i) \in \mathbb{R} \times \{1, 2, 3, 4\}$  is given by Lemma 5.5. Then, we have*

$$F_{J_k} = \begin{cases} (F_{(L,K)}^{(i)})_{T^-(t)} & \text{for } k \in \{1, 2\} \text{ and } i \in \{1, 2, 3, 4\} \\ (F_{(L,K)}^{(i)})_{T^-(-t)} & \text{for } k \in \{3, 4\} \text{ and } i \in \{1, 2\} \\ (F_{(L,K)}^{(j)})_{T^-(-t)} & \text{for } k \in \{3, 4\} \text{ and } i, j \in \{3, 4\} \text{ with } j \neq i. \end{cases}$$

*Proof.* From (5.7), we see that  $J_k$  fixes the forms in  $V_{\mathbb{R},f}^0$  for  $k \in \{1, 2\}$ , and that  $J_k$  acts on the forms in  $V_{\mathbb{R},f}^0$  by changing the sign of the  $x^3y$ -coefficient for  $k \in \{3, 4\}$ . Using (5.12) and (5.13), we then easily verify that the claim holds.  $\square$

**5.3. Reducible case.** Consider  $f(x, y) = \alpha x^2 + \beta xy$ , where  $\alpha, \beta \in \mathbb{N}$ . Although the discussion in Section 5.2 still applies, we shall give an alternative parametrization for the set  $V_{\mathbb{R},f}^0$  in this case. By (3.4), we know that an element in  $V_{\mathbb{R},f}$  is of the form

$$(5.16) \quad F(x, y) = a_4 x^4 + \left( \frac{2\alpha(\beta^2 a_2 - 4\alpha^2 a_0)}{\beta^3} \right) x^3 y + a_2 x^2 y^2 + \left( \frac{4\alpha a_0}{\beta} \right) x y^3 + a_0 y^4.$$

Also, recall (4.16), and for each  $t \in \mathbb{R}$  define

$$T(t) = \begin{pmatrix} e^{-t} & 0 \\ \frac{2\alpha \sinh t}{\beta} & e^t \end{pmatrix},$$

which lies in  $O_f(\mathbb{Z})$ . Note that  $F_{T(t)} \in V_{\mathbb{R},f_0}^0$  for all  $F \in V_{\mathbb{R},f_0}^0$  by Lemmas 4.6 and 4.7.

**Lemma 5.8.** *Let  $F \in V_{\mathbb{R},f}^0$  be as in (5.16) and let  $t \in \mathbb{R}$ . Then, we have*

$$F_{T(t)}(x, y) = A(t)x^4 + (*)x^3y + B(t)x^2y^2 + (*)xy^3 + C(t)y^4,$$

where

$$(5.17) \quad \begin{cases} A(t) = e^{-4t}a_4 + \frac{\alpha^2}{\beta^2}(e^{4t} - 1)e^{-4t}a_2 + \frac{\alpha^4}{\beta^4}(e^{4t} - 1)(e^{4t} - 5)e^{-4t}a_0 \\ B(t) = a_2 + \frac{6\alpha^2}{\beta^2}(e^{4t} - 1)a_0 \\ C(t) = e^{4t}a_0. \end{cases}$$

Moreover, there exists a unique  $t \in \mathbb{R}$  such that  $|C(t)| = \beta^2$ .

*Proof.* The formulae in (5.17) follow from a direct computation. Observe that  $a_0 \neq 0$ , for otherwise  $x^2$  divides  $F(x, y)$  and  $\Delta(F) = 0$ . Thus, clearly  $|C(t)| = \beta^2$  for a unique  $t \in \mathbb{R}$ , namely  $t = \log(\beta^2/|a_0|)/4$ .  $\square$

Lemma 5.8 has the following consequence.

**Lemma 5.9.** *Let  $F \in V_{\mathbb{R},f}^0$  be given, and write  $L = L_f(F)$  and  $K = K_f(F)$ . Then, there exists a unique pair  $(t, i) \in \mathbb{R} \times \{1, 2\}$  such that*

$$F(x, y) = (F_{f,(L,K)}^{(i)})_{T(t)}(x, y),$$

where

$$\begin{aligned} F_{f,(L,K)}^{(i)}(x, y) = & \left( \frac{L^2 + (-1)^i 72\alpha^2 L + 4K + 144\alpha^4}{(-1)^i 144\beta^2} \right) x^4 + \left( \frac{\alpha L + (-1)^i 4\alpha^3}{\beta} \right) x^3 y \\ & + \left( \frac{L + (-1)^i 12\alpha^2}{2} \right) x^2 y^2 + (-1)^i 4\alpha\beta xy^3 + (-1)^i \beta^2 y^4. \end{aligned}$$

*Proof.* Uniqueness follows from Lemma 5.8. As for existence, again by Lemma 5.8 and also (5.16), there exists  $-t \in \mathbb{R}$  such that  $F_{T(-t)}(x, y)$  is of the shape

$$Ax^4 + \left( \frac{2\alpha B - (-1)^i 8\alpha^3}{\beta} \right) x^3 y + Bx^2 y^2 + (-1)^i 4\alpha\beta xy^3 + (-1)^i \beta^2 y^4,$$

where  $i \in \{1, 2\}$ . Using Propositions 3.4 and 3.7, we compute that

$$L = 2B - (-1)^i 12\alpha^2 \text{ and } K = -B^2 + (-1)^i 36\beta^2 A - (-1)^i 24\alpha^2 B + 144\alpha^4.$$

Solving the above, we obtain

$$(A, B) = \left( \frac{L^2 + (-1)^i 72\alpha^2 L + 4K + 144\alpha^4}{(-1)^i 144\beta^2}, \frac{L + (-1)^i 12\alpha^2}{2} \right).$$

It follows that  $F_{T(-t)}(x, y) = F_{f,(L,K)}^{(i)}(x, y)$ , as desired.  $\square$

Recall (1.4), and note that Lemma 5.9 implies that for  $i = 1, 2$ , we have a map

$$\Phi_f^{(i)} : \Omega^0 \times \mathbb{R} \longrightarrow V_{\mathbb{R},f}^0; \quad \Phi_f^{(i)}(L, K, t) = (F_{f,(L,K)}^{(i)})_{T(t)}.$$

Identifying  $V_{\mathbb{R},f}$  with  $\mathbb{R}^3$  via (3.5), we deduce from (5.17) that

$$\Phi_f^{(i)}(L, K, t) = (\Phi_{f,1}^{(i)}(L, K, t), \Phi_{f,2}^{(i)}(L, K, t), \Phi_{f,3}^{(i)}(L, K, t)),$$



where

$$(5.18) \quad \begin{cases} \Phi_{f,1}^{(i)}(L, K, t) = \frac{(-1)^i e^{-4t}}{144\beta^2}(L^2 + 4K) + \frac{\alpha^2}{2\beta^2}L + \frac{(-1)^i \alpha^4 e^{4t}}{\beta^2} \\ \Phi_{f,2}^{(i)}(L, K, t) = \frac{L}{2} + (-1)^i 6\alpha^2 e^{4t} \\ \Phi_{f,3}^{(i)}(L, K, t) = (-1)^i \beta^2 e^{4t}. \end{cases}$$

Note that by Proposition 3.4, the form  $\Phi_f^{(i)}(L, K, t)$  has  $L_f$ - and  $K_f$ -invariants equal to  $L$  and  $K$ , respectively.

**Proposition 5.10.** *For  $i = 1, 2$ , the map  $\Phi_f^{(i)}$  is injective and its Jacobian*

$$\mathfrak{J}_f^{(i)} = \begin{pmatrix} \frac{\partial \Phi_{f,1}^{(i)}}{\partial L} & \frac{\partial \Phi_{f,1}^{(i)}}{\partial K} & \frac{\partial \Phi_{f,1}^{(i)}}{\partial t} \\ \frac{\partial \Phi_{f,2}^{(i)}}{\partial L} & \frac{\partial \Phi_{f,2}^{(i)}}{\partial K} & \frac{\partial \Phi_{f,2}^{(i)}}{\partial t} \\ \frac{\partial \Phi_{f,3}^{(i)}}{\partial L} & \frac{\partial \Phi_{f,3}^{(i)}}{\partial K} & \frac{\partial \Phi_{f,3}^{(i)}}{\partial t} \end{pmatrix}$$

has determinant equal to  $-1/18$ . Moreover, we have

$$(5.19) \quad V_{\mathbb{R},f}^0 = \bigsqcup_{i=1}^2 \Phi_f^{(i)}(\Omega^0 \times \mathbb{R}).$$

*Proof.* That  $\Phi_f^{(i)}$  is an injection and that (5.19) holds follow from Lemma 5.9. As for the claim that  $\det(\mathfrak{J}_f^{(i)}) = -1/18$ , it may be verified by explicit computation.  $\square$

## 6. COUNTING FORMS OF BOUNDED HEIGHT UP TO $\mathrm{GL}_2(\mathbb{Z})$ -EQUIVALENCE

Throughout this section, let  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$  be a primitive form in  $W_{\mathbb{Z}}^0$  with  $\alpha > 0$ . We shall prove an asymptotic formula for the quantity  $N_{\mathbb{Z},f}^0(X)$  defined as in Section 1. In view of the bijection (1.7), without loss of generality, we shall also assume that  $f$  is reduced when  $f$  is positive definite or reducible. This assumption is needed when we use the results in Section 4.3 to determine the value of  $r_f$  in (4.2), and the parametrization of  $V_{\mathbb{R},f}^0$  proved in Section 5.3 when  $f$  is reducible.

In view of the definition of our height, let  $\mathcal{H}(X)$  denote the subset of  $\mathbb{R}^2$  consisting of the pairs  $(L, K)$  with  $\max\{L^2, |K|\} \leq X$ . Recall (5.1), and for  $* \in \{0, +, -\}$  define

$$\Omega^*(X) = \Omega^* \cap \mathcal{H}(X)$$

The case when  $f$  is positive definite is relatively straightforward, since we may take the third parameter  $t$  to lie in the interval  $[-\pi/4, \pi/4)$  by Lemma 5.2. The case when  $f$  is indefinite requires a more nuanced argument, and we shall show that  $t$  may also be restricted to an interval of finite length.

The reader should recall the discussion and notation at the beginning of Section 4.

**6.1. Proof of Theorem 1.2 (a).** Suppose that  $f$  is positive definite and also recall the notation from Section 5.1. We shall take

$$\mathcal{S}_f(X) = (\Psi_f \circ \Phi)(\Omega^+(X) \times [-\pi/4, \pi/4]),$$

where  $\Psi_f$  is as in (4.10). By Proposition 5.3, we see that

$$\mathcal{S}_f(X) = \{F \in V_{\mathbb{R},f}^0 \mid H_f(F) \leq X\}.$$

Identifying  $V_{\mathbb{R},f}$  with  $\mathbb{R}^3$  via (3.2), the above is clearly a semi-algebraic subset of  $V_{\mathbb{R},f}$  by Proposition 3.6.

By (5.6), it is clear that  $\mathcal{R}_f(X)$  is contained in the cube centered at the origin and of side length  $O_f(X^{1/2})$ , and so  $\text{Vol}(\overline{\mathcal{R}_f(X)}) = O_f(X)$ . It then follows from (4.1) and Proposition 4.2 that

$$N_{\mathbb{Z},f}^0(X) = \frac{1}{s_f r_f} \left( \frac{\text{Vol}(\mathcal{S}_f(X))}{\alpha^3} + O_f(X \log X) \right),$$

where  $s_f$  and  $r_f$  are as in (1.8) and (4.2), respectively. Write  $-D$  for the discriminant of  $f$ . Recall that  $\det(\Psi_f) = 8\alpha^3 D^{-3/2}$ , and the Jacobian of  $\Phi$  has determinant  $-1/18$  by Proposition 5.3. Thus, we have

$$\text{Vol}(\mathcal{S}_f(X)) = \frac{4\alpha^3}{9D^{3/2}} \text{Vol}(\Omega^+(X) \times [-\pi/4, \pi/4]).$$

We compute that

$$\text{Vol}(\Omega^+(X) \times [-\pi/4, \pi/4]) = \int_{-X^{1/2}}^{X^{1/2}} \int_{-L^2/4}^X \frac{\pi}{2} dK dL = \frac{13\pi}{12} X^{3/2}.$$

From here, we see that it remains to determine the value of  $r_f$ .

**Lemma 6.1.** *Under the assumption that  $f$  is reduced, we have*

$$r_f = \begin{cases} 1 & \text{if } f \text{ is not ambiguous} \\ 6 & \text{if } f(x, y) = x^2 + xy + y^2 \\ 2 & \text{otherwise.} \end{cases}$$

*Proof.* Notice that  $V_{\mathbb{Z},f}^0(X) \subset \mathcal{S}_f(X)$  and let  $F \in \mathcal{S}_f(X)$  be any integral form having non-square discriminant. Then, we have  $r_f = [O_f(\mathbb{Z}) : \text{Stab}_{O_f(\mathbb{Z})}(F)]$ . We then deduce from Corollary 4.9 and Proposition 4.11 that  $r_f$  is as stated.  $\square$

**6.2. Proof of Theorem 1.3 (a).** Suppose that  $f$  is reducible, so  $\gamma = 0$  and  $\beta > 0$ . Also, recall the notation from Section 5.3 and Proposition 5.10.

**Lemma 6.2.** *Let  $F \in V_{\mathbb{Z},f}^0(X)$  be given, and write  $L = L_f(F)$  and  $K = K_f(F)$ . Also, let  $(t, i) \in \mathbb{R} \times \{1, 2\}$  be the pair such that  $F = \Phi_f^{(i)}(L, K, t)$ . Then, we have*

$$(6.1) \quad 1 \leq |8C_F/\beta^2| \leq 20X/9,$$

where  $C_F$  denotes the  $y^4$ -coefficient of  $F$ , and the above is equivalent to

$$-(\log 8)/4 \leq t \leq \log(5X/18)/4.$$

*Proof.* Since  $\alpha$  and  $\beta$  are coprime, by considering the  $x^3y$ -coefficient of  $F$ , we deduce from (5.16) that  $8C_F/\beta^2 \in \mathbb{Z}$ . Also, note that  $4(L^2 + 4K)/9$  is non-zero by (1.4) and is divisible by  $8C_F/\beta^2$  by Proposition 3.7. Since  $\max\{L^2, |K|\} \leq X$ , we see that (6.1) holds. Notice that  $|C_F| = \beta^2 e^{4t}$  by (5.18), so clearly (6.1) is equivalent to the stated bounds for  $t \in \mathbb{R}$ .  $\square$

In view of Lemma 6.2, put

$$t_{f,1} = -(\log 8)/4 \text{ and } t_{f,2} = \log(5X/18)/4.$$

We shall then take

$$\mathcal{S}_f(X) = \bigsqcup_{i=1}^2 \Phi_f^{(i)}(\Omega^0(X) \times [t_{f,1}, t_{f,2}])$$

By Proposition 5.10 and Lemma 6.2, we see that

$$\mathcal{S}_f(X) = \{F \in V_{\mathbb{R},f}^0 \mid H_f(F) \leq X \text{ and (6.1)}\}.$$

Identifying  $V_{\mathbb{R},f}$  with  $\mathbb{R}^3$  via (3.5), the above is clearly a semi-algebraic subset of  $V_{\mathbb{R},f}$  by Proposition 3.7.

By (5.18) and the bound on  $t \in \mathbb{R}$ , it is clear that  $\mathcal{R}_f(X)$  is contained in the cube centered at the origin and of side length  $O_f(X)$ . Thus, the projection of  $\mathcal{R}_f(X)$  onto any coordinate subspace by equating two coordinates to zero has length  $O_f(X)$ . That of  $\mathcal{R}_f(X)$  onto a coordinate subspace by equating one coordinate to zero needs to be dealt with using a different argument.

**Lemma 6.3.** *For each  $j = 1, 2, 3$ , let  $\mathcal{R}_f(X)_j$  denote the projection of  $\mathcal{R}_f(X)$  onto the coordinate subspace by equating the  $j$ -th coordinate to zero. Then, we have*

$$\text{Vol}(\mathcal{R}_f(X)) = O_f(X^{3/2}).$$

*Proof.* Let  $\mathcal{S}_f(X)_j$  be the projection of  $\mathcal{S}_f(X)$  onto the coordinate subspace by equating the  $j$ -th coordinate to zero. Since  $\mathcal{L}_{f,\beta}$  depends only upon  $f$ , it is enough to show that  $\text{Vol}(\mathcal{S}_f(X)) = O_f(X^{3/2})$ . Recall that we identify  $V_{\mathbb{R},f}$  with  $\mathbb{R}^3$  via (3.5).

Consider a tuple  $(A, B, C) \in \mathcal{S}_f(X)$ , the image of  $(L, K, t) \in \Omega^0(X) \times [t_{f,1}, t_{f,2}]$  under  $\Phi_f$  say, so  $(A, B, C)$  is given by (5.18). We have  $(-1)^i e^{4t} = C/\beta^2$ , as well as

$$|B - 6\alpha^2 C/\beta^2| \leq \frac{1}{2}X^{1/2} \text{ and } |A - \alpha^4 C/\beta^4| \leq \frac{5}{144|C|}X + \frac{\alpha^2}{2\beta^2}X^{1/2}$$

since  $\max\{L^2, |K|\} \leq X$ . It follows that

$$\text{Vol}(\mathcal{S}_f(X)_1) \leq 2 \int_{\beta^2/8}^{5\beta^2 X/18} X^{1/2} dC = O_f(X^{3/2})$$

and similarly

$$\text{Vol}(\mathcal{S}_f(X)_2) \leq 2 \int_{\beta^2/8}^{5\beta^2 X/18} \left( \frac{5}{72C}X + \frac{\alpha^2}{\beta^2}X^{1/2} \right) dC = O_f(X^{3/2}).$$

Finally, again by (5.18), we have  $(-1)^i e^{4t} = (2B - L)/(12\alpha^2)$ . We then find that

$$|A - (\alpha^2 B)/(6\beta^2)| \leq \frac{5\alpha^2}{12\beta^2} \frac{1}{|2B - L|}X + \frac{5\alpha^2}{12\beta^2}X^{1/2}$$

since  $\max\{L^2, |K|\} \leq X$ . By the bound on  $t \in \mathbb{R}$ , we also know that

$$3\alpha^2/2 \leq |2B - L| \leq 10\alpha^2 X/3 \text{ and so } |B| \leq 5\alpha^2 X/3 + X^{1/2}/2.$$

Using the bounds

$$\frac{1}{|2B - L|} \leq \begin{cases} \frac{1}{-2B - X^{1/2}} & \text{for } -\frac{5\alpha^2 X}{3} - \frac{X^{1/2}}{2} \leq B \leq -\frac{3\alpha^2}{4} - \frac{X^{1/2}}{2} \\ \frac{2}{3\alpha^2} & \text{for } -\frac{X^{1/2}}{2} - \frac{3\alpha^2}{4} \leq B \leq \frac{X^{1/2}}{2} + \frac{3\alpha^2}{4} \\ \frac{1}{2B - X^{1/2}} & \text{for } \frac{3\alpha^2}{4} + \frac{X^{1/2}}{2} \leq B \leq \frac{5\alpha^2 X}{3} + \frac{X^{1/2}}{2}, \end{cases}$$

we then deduce that

$$\text{Vol}(\mathcal{S}_f(X)_3) \leq 2 \int_{3\alpha^2/4 + X^{1/2}/2}^{5\alpha^2 X/3 + X^{1/2}/2} \left( \frac{5\alpha^2}{12\beta^2} \frac{X}{2B - X^{1/2}} \right) dB + O_f(X^{3/2}) = O_f(X^{3/2}).$$

This completes the proof of the lemma.  $\square$

We now deduce from (4.1) and Proposition 4.2 that

$$N_{\mathbb{Z},f}^0(X) = \frac{1}{s_f r_f} \left( \frac{8 \text{Vol}(\mathcal{S}_f(X))}{\beta^3} + O_f(X^{3/2}) \right),$$

where  $s_f$  and  $r_f$  are defined as in (1.8) and (4.2), respectively. The Jacobian of  $\Phi_f^{(i)}$  has determinant  $-1/18$  by Proposition 5.10, and so we have

$$\text{Vol}(\mathcal{S}_f(X)) = \text{Vol}(\Omega^0(X) \times [t_{f,1}, t_{f,2}])/9.$$

We compute that

$$\text{Vol}(\Omega^0(X) \times [t_{f,1}, t_{f,2}]) = \int_{-X^{1/2}}^{X^{1/2}} \int_{-X}^X \frac{1}{4} \log \left( \frac{20X}{9} \right) dK dL = X^{3/2} \log(20X/9).$$

Note that  $f$  has discriminant  $\beta^2$ . From here, we see that it remains to determine  $r_f$ .

**Lemma 6.4.** *Under the assumption that  $f$  is reduced, we have*

$$r_f = \begin{cases} 1 & \text{if } \beta \nmid \alpha^2 + 1 \text{ and } \beta \nmid \alpha^2 - 1 \\ 2 & \text{otherwise.} \end{cases}$$

*Proof.* Notice that  $V_{\mathbb{Z},f}^0(X) \subset \mathcal{S}_f(X)$  and let  $F \in \mathcal{S}_f(X)$  be any integral form having non-square discriminant. Then, we have  $r_f = [O_f(\mathbb{Z}) : \text{Stab}_{O_f(\mathbb{Z})}(F)]$ . We then deduce from Corollary 4.9 and Proposition 4.12 that  $r_f$  is as stated.  $\square$

**6.3. Proof of Theorem 1.4 (a).** Suppose that  $f$  is indefinite and irreducible. Let  $D$  be the discriminant of  $f$  and let  $t_D > 0$  be defined as in (1.9). Recall the notation from Section 5.2, and we shall take

$$(6.2) \quad \mathcal{S}_f(X) = \Psi_f \left( \bigsqcup_{i=1}^2 \Phi^{(i)}(\Omega^+(X) \times [0, t_D]) \sqcup \bigsqcup_{i=3}^4 \Phi^{(i)}(\Omega^-(X) \times [0, t_D]) \right),$$

where  $\Psi_f$  is as in (4.10). Below, we shall verify that  $\mathcal{S}_f(X)$  is indeed a semi-algebraic subset of  $V_{\mathbb{R},f}$ . To that end, recall Proposition 3.6. Given  $F \in V_{\mathbb{R},f}^0$ , define

$$E_{f,1}(F) = L_{f,1}(F) - \sqrt{D}L_{f,2}(F) \text{ and } E_{f,2}(F) = L_{f,1}(F) + \sqrt{D}L_{f,2}(F),$$

both of which are non-zero by (1.4). In particular, they have the same sign precisely when  $\Delta(F) > 0$ . It will also be helpful to recall Proposition 5.6. Then, we have:

**Lemma 6.5.** *Let  $F \in V_{\mathbb{R},f}^{0,+}$  be given, and write  $L = L_f(F)$  and  $K = K_f(F)$ . Further, let  $(t, i) \in \mathbb{R} \times \{1, 2\}$  be the pair such that  $F = \Psi_f(\Phi^{(i)}(L, K, t))$ . Write  $E_1 = E_{f,1}(F)$  and  $E_2 = E_{f,2}(F)$ . Then, the condition that  $0 \leq t < t_D$  is equivalent to*

$$(6.3) \quad |E_2| \leq |E_1| < e^{8t_D} |E_2|.$$

*Proof.* Using (4.11) and (5.12), we compute that

$$E_1 = (-1)^i 2\alpha^2 \sqrt{L^2 + 4K} e^{4t} / 3 \text{ and } E_2 = (-1)^i 2\alpha^2 \sqrt{L^2 + 4K} e^{-4t} / 3.$$

It follows that  $E_1/E_2 = e^{8t}$ , and so  $0 \leq t < t_D$  is equivalent to (6.3).  $\square$

**Lemma 6.6.** *Let  $F \in V_{\mathbb{R},f}^{0,-}$  be given, and write  $L = L_f(F)$  and  $K = K_f(F)$ . Further, let  $(t, i) \in \mathbb{R} \times \{3, 4\}$  be the pair such that  $F = \Psi_f(\Phi^{(i)}(L, K, t))$ . Write  $E_1 = E_{f,1}(F)$  and  $E_2 = E_{f,2}(F)$ . Also, put*

$$Z = Z_f(F) = (L^2 + 4K) / (3L - (-1)^i 2\sqrt{2L^2 - K})^2.$$

*Then, the condition that  $0 \leq t < t_D$  is equivalent to*

$$(6.4) \quad |E_2| \leq |E_1 Z| < e^{8t_D} |E_2|.$$

*Moreover, the region defined by (6.4) is definable by finitely many polynomial inequalities in the coefficients of  $F$ ; the number of inequalities and their degrees are absolutely bounded.*

*Proof.* Using (4.11) and (5.13), we compute that

$$\begin{aligned} E_1 &= -2\alpha^2 (3L - (-1)^i 2\sqrt{2L^2 - K}) e^{4t} / 3 \\ E_2 &= -2\alpha^2 (3L + (-1)^i 2\sqrt{2L^2 - K}) e^{-4t} / 3. \end{aligned}$$

It follows that  $E_1 Z / E_2 = e^{8t}$  and so  $0 \leq t < t_D$  is equivalent to (6.4).

Next, observe that  $L^2 + 4K < 0$  implies that

$$Z < 0, \quad E_1 E_2 < 0, \quad 3L - 2\sqrt{2L^2 - K} < 0.$$

It follows that (6.4) may be rewritten as

$$\begin{cases} E_2 \leq E_1 Z < e^{8t_D} E_2 & \text{if } E_2 > 0, \text{ which is equivalent to } i = 3 \\ E_2 \geq E_1 Z > e^{8t_D} E_2 & \text{if } E_2 < 0, \text{ which is equivalent to } i = 4. \end{cases}$$

For brevity, we shall also use the notation

$$\begin{aligned} Y_1 &= Y_1(F) = -E_1(L^2 + 4K) + E_2(17L^2 - 4K) \\ Y_2 &= Y_2(F) = -E_1(L^2 + 4K) + e^{8t_D} E_2(17L^2 - 4K). \end{aligned}$$

By rearranging, we may then write (6.4) as

$$(6.5) \quad 12E_2 L \sqrt{2L^2 - K} \leq (-1)^i Y_1 \text{ and } 12e^{8t_D} E_2 L \sqrt{2L^2 - K} > (-1)^i Y_2.$$

Note that  $E_1, E_2, L, K, Y_1$ , and  $Y_2$  are polynomials in the coefficients of  $F$ . By considering various possibilities for the signs of  $E_2, L, Y_1$ , and  $Y_2$ , we then see that (6.4) is definable by finitely many polynomial inequalities. For example, when  $E_2 > 0$  and  $L \geq 0$ , we have that (6.5) is equivalent to  $Y_1 \leq 0$  together with

$$\begin{cases} (12E_2L)^2(2L^2 - K) \leq Y_1^2 & \text{if } Y_2 > 0 \\ (12E_2L)^2(2L^2 - K) \leq Y_1^2 \text{ and } (12e^{8t_D}E_2L)^2(2L^2 - K) > Y_2^2 & \text{if } Y_2 \leq 0. \end{cases}$$

The other cases are analogous. It is clear that the number of inequalities needed and their degrees are absolutely bounded. This completes the proof.  $\square$

By Propositions 5.6, as well as Lemmas 6.5 and 6.6, we see that

$$(6.6) \quad \mathcal{S}_f(X) = \{F \in V_{\mathbb{R},f}^0 \mid H_f(F) \leq X, \Delta(F) > 0, \text{ and (6.3)}\} \\ \cup \{F \in V_{\mathbb{R},f}^0 \mid H_f(F) \leq X, \Delta(F) < 0, \text{ and (6.4)}\}.$$

Identifying  $V_{\mathbb{R},f}$  with  $\mathbb{R}^3$  via (3.2), we then see that  $\mathcal{S}_f(X)$  is indeed a semi-algebraic subset of  $V_{\mathbb{R},f}$  by Proposition 3.6 and Lemma 6.6.

By (5.12) and (5.13), as well as the bound on  $t \in \mathbb{R}$ , clearly  $\mathcal{R}_f(X)$  is contained in the cube centered at the origin and of side length  $O_f(X^{1/2})$ , so  $\text{Vol}(\overline{\mathcal{R}_f(X)}) = O_f(X)$ . We then deduce from (4.1) and Proposition 4.2 that

$$N_{\mathbb{Z},f}^0(X) = \frac{1}{s_f r_f} \left( \frac{\text{Vol}(\mathcal{S}_f(X))}{\alpha^3} + O_f(X \log X) \right),$$

where  $s_f$  and  $r_f$  are as in (1.8) and (4.2), respectively. Because  $\det(\Psi_f) = 8\alpha^3 D^{-3/2}$ , and the Jacobian of  $\Phi^{(i)}$  has determinant  $-1/18$  by Proposition 5.6, we have

$$\text{Vol}(\mathcal{S}_f(X)) = \frac{8\alpha^3}{9D^{3/2}} \left( \text{Vol}(\Omega^+(X) \times [0, t_D]) + \text{Vol}(\Omega^-(X) \times [0, t_D]) \right).$$

We compute that

$$\begin{aligned} \text{Vol}(\Omega^+(X) \times [0, t_D]) &= \int_{-X^{1/2}}^{X^{1/2}} \int_{-L^2/4}^X t_D dK dL = \frac{13t_D}{6} X^{3/2} \\ \text{Vol}(\Omega^-(X) \times [0, t_D]) &= \int_{-X^{1/2}}^{X^{1/2}} \int_{-X}^{-L^2/4} t_D dK dL = \frac{11t_D}{6} X^{3/2}. \end{aligned}$$

It remains to show that  $\mathcal{S}_f(X)$  contains at least one representative from each  $\text{GL}_2(\mathbb{Z})$ -equivalence class of the forms in  $V_{\mathbb{Z},f}^0(X)$ , and to determine  $r_f$  given in (4.2).

Let  $F \in V_{\mathbb{Z},f}^0(X)$  be given, and write  $L = L_f(F)$  and  $K = K_f(F)$ . Then, by (4.10) as well as Proposition 5.6, there exists  $(t, i) \in \mathbb{R} \times \{1, 2, 3, 4\}$  such that

$$(6.7) \quad F = (F_{(L,K)}^{(i)})_{T^-(t)T_f}.$$

Now, recall the notation in (4.17) and (5.15). Observe that by the definition of  $t_D > 0$  and (4.16), we have  $T_D = T_f^{-1} J_k T^-(t_D) T_f$ , where  $k = 2$  if  $D$  is of negative type, and  $k = 1$  otherwise. Also, for any  $n \in \mathbb{Z}$ , we have

$$T_D^n = T_f^{-1} J_k^n T^-(nt_D) T_f,$$

which lies in  $O_f(\mathbb{Z})$  by Proposition 4.13. But

$$F_{T_D^n} = (F_{(L,K)}^{(i)})_{T^-(t+nt_D)T_f}$$

by Lemma 5.7, and we may choose  $n \in \mathbb{Z}$  to be such that  $0 \leq t + nt_D < t_D$ . Hence, indeed  $F$  is  $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to a form in  $\mathcal{S}_f(X)$ . Further, note that for  $0 \leq t < t_D$ , we have  $0 \leq t + nt_D < t_D$  if and only if  $n = 0$ , namely  $T_D^n = I_{2 \times 2}$ . So, for  $F \in \mathcal{S}_f(X)$ , the above also shows that  $F$  is not  $G_f(\mathbb{Z})$ -equivalent to any form in  $\mathcal{S}_f(X) \setminus \{F\}$ .

**Lemma 6.7.** *We have*

$$r_f = \begin{cases} 1 & \text{if } f \text{ is neither ambiguous nor opaque} \\ 2 & \text{otherwise.} \end{cases}$$

*Proof.* Let  $F \in \mathcal{S}_f(X)$  be an integral form having non-square discriminant. We have already shown above that  $F$  is not  $G_f(\mathbb{Z})$ -equivalent to any form in  $\mathcal{S}_f(X) \setminus \{F\}$ . So, if  $f$  is neither ambiguous nor opaque, then  $O_f(\mathbb{Z}) = G_f(\mathbb{Z})$  by Proposition 4.13 and thus  $r_f = 1$ . If  $f$  is ambiguous or opaque, then in view of the bijection 1.7, we may assume that  $\alpha$  divides  $\beta$  or  $\alpha = -\gamma$ , respectively.

Let  $M \in O_f(\mathbb{Z})$  be defined as in (4.20) and recall (5.15). Since  $M$  has finite order, we know from (4.18) and (4.19) that there exists  $t_f \in \mathbb{R}$  such that

$$M = \pm T_f^{-1} J_\ell T^-(t_f) T_f,$$

where  $\ell = 3$  if  $\det(M) = 1$ , and  $\ell = 4$  if  $\det(M) = -1$ . Now, by Proposition 4.13, an element  $T \in O_f(\mathbb{Z}) \setminus G_f(\mathbb{Z})$  has finite order is of the form

$$T = \pm M T_D^n = \pm M T_f^{-1} J_k^n T^-(nt_D) T_f$$

for  $n \in \mathbb{Z}$ , where  $k = 2$  if  $D$  is of negative type, and  $k = 1$  otherwise. Hence, we have

$$T = \pm T_f^{-1} J_\ell T^-(t_f) J_k^n T^-(nt_D) T_f.$$

Using the same notation as in (6.7), we then deduce from Lemma 5.7 that

$$\begin{aligned} F_T &= (F_{(L,K)}^{(i)})_{T^-(t)J_\ell T^-(t_f+nt_D)T_f} \\ &= \begin{cases} (F_{(L,K)}^{(i)})_{T^-(t-t_f+nt_D)T_f} & \text{for } i \in \{1, 2\} \\ (F_{(L,K)}^{(j)})_{T^-(t-t_f+nt_D)T_f} & \text{for } i, j \in \{3, 4\} \text{ with } j \neq i. \end{cases} \end{aligned}$$

We may choose  $n \in \mathbb{Z}$  so that  $0 \leq -t + t_f + nt_D < t_D$ , or equivalently  $F_T \in \mathcal{S}_f(X)$ . This  $n \in \mathbb{Z}$  is unique, for if there are two distinct such values  $n_1, n_2 \in \mathbb{Z}$ , then  $F_{MT_D^{n_1}}$  and  $F_{MT_D^{n_2}}$  are distinct forms in  $\mathcal{S}_f(X)$  that are  $G_f(\mathbb{Z})$ -equivalent, which is impossible. Using (4.16), it may be checked that  $T$  is not of the form  $\lambda \begin{pmatrix} \beta & 2\gamma \\ -2\alpha & -\beta \end{pmatrix}$  for any  $\lambda \in \mathbb{R}^\times$ , and hence  $F_T \neq F$  by Corollary 4.9. We have thus shown that there are precisely two representatives from the  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence class of  $F$ , namely  $F$  and  $F_T$ , in  $\mathcal{S}_f(X)$ . Hence, indeed  $r_f = 2$ .  $\square$

## 7. ESTIMATING THE NUMBER OF FORMS OF SQUARE DISCRIMINANTS

Throughout this section, let  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$  be a primitive form in  $W_{\mathbb{Z}}^0$  with  $\alpha > 0$ . Our goal is to give an upper bound for the quantity  $N_{\mathbb{Z}, f}^{\mathrm{sq}}(X)$  defined as in Section 1.



Let  $\mathcal{S}_f(X)$  denote the subset of  $V_{\mathbb{R},f}^0(X)$  defined as in the proof of Theorems 1.2, 1.3, and 1.4 (a), which contains at least one representative from each  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence class of the forms in  $V_{\mathbb{Z},f}^0(X)$ . Since we only need an upper bound, it suffices to count the number of integral forms in  $\mathcal{S}_f(X)$  having square discriminants; the bound for  $N_{\mathbb{Z},f}^{\mathrm{sq}}(X)$  stated in Theorems 1.2, 1.3, and 1.4 (b) is in fact a bound for this number. We recall that  $V_{\mathbb{Z},f}^0(X) \subset \mathcal{S}_f(X)$  when  $f$  is positive definite or reducible.

Consider a form  $F \in V_{\mathbb{Z},f}^0(X)$ . By (1.4) and Proposition 3.5, we know that  $\Delta(F)$  is a square if and only if  $(L_f(F)^2 + 4K_f(F))/9$  is a square. Let  $\mathcal{D}$  denote the discriminant of  $f$  and recall from Proposition 3.6 that

$$(7.1) \quad 4\alpha^4(L_f(F)^2 + 4K_f(F))/9 = L_{f,1}(F)^2 - \mathcal{D}L_{f,2}(F)^2,$$

which is an integer by Proposition 3.5. It is also non-zero by (1.4) since  $\Delta(F) \neq 0$ , and is bounded above by  $20\alpha^2 X/9$  in absolute value.

Now, we know that  $L_f(F) \in \mathbb{Z}$  again by Proposition 3.5, and so there are  $O(X^{1/2})$  choices for  $L_f(X)$ . Since  $L_{f,1}(F), L_{f,2}(F) \in \mathbb{Z}$  by definition, we see from Lemma 7.1 below that it is enough to count the number of possible pairs  $(L_{f,1}(F), L_{f,2}(F))$  in  $\mathbb{Z}^2$  as  $F$  ranges over  $\mathcal{S}_f(X) \cap V_{\mathbb{Z},f}^{\mathrm{sq}}(X)$ .

By extending the definitions of  $L_{f,1}(-)$ ,  $L_{f,2}(-)$ , and  $L_f(-)$  from  $V_{\mathbb{R},f}^0$  to  $V_{\mathbb{R},f}$  via the formulae given in Proposition 3.6, we have the following.

**Lemma 7.1.** *The map  $F \mapsto (L_{f,1}(F), L_{f,2}(F), L_f(F))$  is a bijection from  $V_{\mathbb{R},f}$  to  $\mathbb{R}^3$ .*

*Proof.* Identifying  $V_{\mathbb{R},f}$  with  $\mathbb{R}^3$  via (3.2), the stated map is given by the matrix

$$\begin{pmatrix} 4(\beta^2 - \alpha\gamma) & -3\alpha\beta & 2\alpha^2 \\ 4\beta & -2\alpha & 0 \\ -\frac{6\gamma}{\alpha} & \frac{3\beta}{2\alpha} & -1 \end{pmatrix},$$

which has determinant  $8\alpha\mathcal{D} \neq 0$  and hence is invertible.  $\square$

In the sequel, we shall write  $\sigma_0(-)$  for the divisor function, namely  $\sigma_0(n)$  denotes the number of positive divisors of  $n$  for each  $n \in \mathbb{N}$ . Also, we shall write  $D$  for the absolute value of  $\mathcal{D}$ .

**7.1. Proof of Theorem 1.3 (b).** Suppose that  $f$  is reducible, in which case  $D$  is a square in  $\mathbb{Z}$ . As noted in (7.1), for each  $F \in V_{\mathbb{Z},f}^{\mathrm{sq}}(X)$ , the pair  $(L_{f,1}(F), L_{f,2}(F)) \in \mathbb{Z}^2$  is a solution to  $(x + \sqrt{D}y)(x - \sqrt{D}y) = z^2$  for some  $z \in \mathbb{N}$  with  $z \leq 2\alpha^2 X^{1/2}$ . In view of this, for each  $z \in \mathbb{N}$ , put

$$\mathfrak{N}_f(z) = \#\{(x, y) \in \mathbb{Z}^2 \mid (x + \sqrt{D}y)(x - \sqrt{D}y) = z^2\}.$$

Also, notice that if  $(x, y)$  is an integral solution to  $(x + \sqrt{D}y)(x - \sqrt{D}y) = z^2$ , then

$$x + \sqrt{D}y = d \text{ and } x - \sqrt{D}y = d'$$

for some divisor  $d$  of  $z^2$  and  $d' = z^2/d$ . In particular, we have

$$(x, y) = \left( \frac{d + d'}{2}, \frac{d - d'}{2\sqrt{D}} \right).$$

Taking the sign of  $d$  into account, this implies that  $\mathfrak{N}_f(z) \leq 2\sigma_0(z^2) \leq 2\sigma_0(z)^2$ . Thus, the number of pairs  $(L_{f,1}(F), L_{f,2}(F)) \in \mathbb{Z}^2$  for  $F \in V_{\mathbb{Z},f}^{\text{sq}}(X)$  is bounded above by

$$\sum_{z=1}^{\lfloor 2\alpha^2 X^{1/2} \rfloor} \mathfrak{N}_f(z) \leq 2 \sum_{z=1}^{\lfloor 2\alpha^2 X^{1/2} \rfloor} \sigma_0(z)^2 = O_f(X^{1/2}(\log X)^3).$$

The last equality follows from a well-known result that was stated by Ramanujan in [12] and was proved by Wilson in [15]. Since there are  $O(X^{1/2})$  choices for  $L_f(F) \in \mathbb{Z}$ , we now deduce from Lemma 7.1 that  $N_{\mathbb{Z},f}^{\text{sq}}(X) = O_f(X(\log X)^3)$ , as desired.

**7.2. Proof of Theorems 1.2 and 1.4 (b).** Suppose that  $f$  is irreducible. First, we make the following observation.

**Lemma 7.2.** *Let  $(x, y, z)$  be an integral solution to  $x^2 - \mathcal{D}y^2 = z^2$  with  $z \neq 0$ . Then, either  $x = z$ , or there exist  $p, q, n, d \in \mathbb{Z}$  with  $q, n, d \neq 0$  and  $d \mid 2\mathcal{D}$  such that*

$$(7.2) \quad (x, y, z) = \left( \frac{(\mathcal{D}p^2 + q^2)n}{d}, \frac{2pqn}{d}, \frac{(\mathcal{D}p^2 - q^2)n}{d} \right).$$

*Proof.* Observe that  $(u, v) = (x/z, y/z)$  is a rational solution to  $u^2 - \mathcal{D}v^2 = 1$ . Suppose that  $x \neq z$ , meaning that  $(u, v) \neq (1, 0)$ . Let  $m \in \mathbb{Q}$  denote the slope of the line going through  $(u, v)$  and  $(1, 0)$ , say  $m = p/q$  with  $\gcd(p, q) = 1$ . We then solve that

$$\left( \frac{x}{z}, \frac{y}{z} \right) = \left( \frac{\mathcal{D}p^2 + q^2}{\mathcal{D}p^2 - q^2}, \frac{2pq}{\mathcal{D}p^2 - q^2} \right).$$

Put  $d = \gcd(\mathcal{D}p^2 - q^2, \mathcal{D}p^2 + q^2)$ , which divides  $2\mathcal{D}$  since  $p$  and  $q$  are coprime. Since

$$(x, y) = \left( \frac{(\mathcal{D}p^2 + q^2)/d}{(\mathcal{D}p^2 - q^2)/d} \cdot z, \frac{2pq}{\mathcal{D}p^2 - q^2} \cdot z \right)$$

and  $x \in \mathbb{Z}$ , we must have  $z = (\mathcal{D}p^2 - q^2)n/d$  for some non-zero  $n \in \mathbb{Z}$ , and the claim now follows.  $\square$

Consider  $F \in V_{\mathbb{Z},f}^{\text{sq}}(X) \cap \mathcal{S}_f(X)$ . As noted in (7.1), the pair  $(L_{f,1}(F), L_{f,2}(F)) \in \mathbb{Z}^2$  is a solution to  $x^2 - \mathcal{D}y^2 = z^2$  for some  $z \in \mathbb{N}$  with  $z \leq 2\alpha^2 X^{1/2}$ . So, for  $L_{f,1}(F) = z$ , there are  $\lfloor 2\alpha^2 X^{1/2} \rfloor$  solutions. For  $L_{f,1}(F) \neq z$ , let  $p, q, n, d \in \mathbb{Z}$  be as in Lemma 7.2. Since  $n$  divides  $z$ , we must have

$$(7.3) \quad 1 \leq |n| \leq 2\alpha^2 X^{1/2}.$$

Further, we claim that there exists a constant  $\mathcal{B}_f$  depending only on  $f$  such that

$$(7.4) \quad |(Dp^2 + q^2)n/d| \leq \mathcal{B}_f X^{1/2}.$$

If  $f$  is positive definite, take  $\mathcal{B}_f = 2\alpha^2$  and (7.4) follows by looking at the  $z$ -coordinate in (7.2). If  $f$  is indefinite, note that by the bound of  $t \in \mathbb{R}$  in the definition of  $\mathcal{S}_f(X)$ , as well as (4.11) and (5.12), the coefficients of  $F$  are all of order  $O_f(X^{1/2})$ . This shows that  $L_{f,1}(X) = O_f(X^{1/2})$ , and (7.4) follows by looking at the  $x$ -coordinate in (7.2).

In view of this, for each positive divisor  $d$  of  $2\mathcal{D}$ , put

$$\mathfrak{N}_f(d, X) = \#\{(p, q, n) \in \mathbb{Z}^3 \mid (7.3) \text{ and } (7.4)\}.$$

Then, by the discussion above, we see that the number of pairs  $(L_{f,1}(F), L_{f,2}(F)) \in \mathbb{Z}^2$  for  $F \in \mathcal{S}_f(X) \cap V_{\mathbb{Z},f}^{\text{sq}}(X)$  is bounded above by

$$2\alpha^2 X^{1/2} + \sum_{d \mid 2\mathcal{D}} \mathfrak{N}_f(d, X).$$

Now, fix  $d \mid 2\mathcal{D}$  and  $n \in \mathbb{Z}$  with  $n \neq 0$ . Then (7.4) defines an ellipse, and the number of points  $(p, q) \in \mathbb{Z}^2$  inside it is of order  $O_f(X^{1/2}/|n|)$ . Summing over  $n$ , we obtain

$$\mathfrak{N}_f(d, X) = O_f \left( X^{1/2} \int_1^{2\alpha^2 X^{1/2}} \frac{1}{n} dn \right) = O_f(X^{1/2} \log X),$$

Since there are  $O(X^{1/2})$  choices for  $L_f(F)$ , we deduce from Lemma 7.1 and the above that  $N_{\mathbb{Z},f}^{\text{sq}}(X) = O_f(\sigma_0(2\mathcal{D})X \log X) = O_f(X \log X)$ , as claimed.

## 8. ESTIMATING THE NUMBER OF REDUCIBLE FORMS

Throughout this section, let  $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$  be a primitive form in  $W_{\mathbb{Z}}^0$  with  $\alpha > 0$ . Our goal is to give an upper bound for the quantity  $N_{\mathbb{Z},f}^{\text{red}}(X)$  defined as in Section 1.

**8.1. Reducibility types.** There are only two reducibility types for the forms in  $V_{\mathbb{Z},f}^0$ . To prove this, first we make the following observations. In the sequel, write  $\mathcal{D}$  for the discriminant of  $f$ . It will also be helpful to recall the notation in (1.2) and (1.3).

**Lemma 8.1.** *Let  $\ell(x, y) = \ell_1 x + \ell_0 y$ , where  $(\ell_1, \ell_0) \in \mathbb{C}^2 \setminus \{\mathbf{0}\}$ . Suppose that  $\ell_{M_f} = \tau \cdot \ell$  for some  $\tau \in \mathbb{C}^\times$ . Then, we have  $\tau = \pm\sqrt{-1}$ , and there exists  $\lambda \in \mathbb{C}^\times$  such that*

$$(8.1) \quad (\ell_1, \ell_0) = \lambda(2\alpha, \beta - \tau\sqrt{-\mathcal{D}}) \text{ or } (\ell_1, \ell_0) = \lambda(\beta + \tau\sqrt{-\mathcal{D}}, 2\gamma).$$

*Proof.* Since  $\ell_{M_f} = \tau \cdot \ell$  and  $\det(M_f) = -\mathcal{D}$ , a simple calculation shows that  $(\ell_1, \ell_0)^T$  is an eigenvector with corresponding eigenvalue  $\tau$  of the transpose of  $M_f$  multiplied by the scalar  $1/\sqrt{-\mathcal{D}}$ . This matrix has characteristic polynomial  $X^2 + 1$ , so  $\tau = \pm\sqrt{-1}$ . By computing the eigenspaces, we see that  $(\ell_1, \ell_0)$  has the form (8.1).  $\square$

**Lemma 8.2.** *Let  $p(x, y) = p_2 x^2 + p_1 xy + p_0 y^2$ , where  $(p_2, p_1, p_0) \in \mathbb{C}^3 \setminus \{\mathbf{0}\}$ . Suppose that  $p_{M_f} = \tau \cdot p$  for some  $\tau \in \mathbb{C}^\times$ . Then, we have  $\tau = \pm 1$ , and*

$$\tau = \begin{cases} -1 & \text{if and only if } p_0 = (\beta p_1 - 2\gamma p_2)/(2\alpha) \\ 1 & \text{if and only if } p = (p_2/\alpha)f. \end{cases}$$

*Proof.* Since  $(M_f)^2 = \mathcal{D}I_{2 \times 2}$  leaves  $p$  invariant, that  $p_{M_f} = \tau \cdot p$  implies  $p = \tau^2 \cdot p$  and so  $\tau = \pm 1$ . Note that  $p(\beta x + 2\gamma y, -2\alpha x - \beta y) = -\tau \mathcal{D}p(x, y)$  since  $\det(M_f) = -\mathcal{D}$ . Now, a simple calculation shows that

$$\begin{aligned} p(\beta x + 2\gamma y, -2\alpha x - \beta y) &= (\beta^2 p_2 - 2\alpha\beta p_1 + 4\alpha^2 p_0)x^2 \\ &\quad + (4\beta\gamma p_2 - (\beta^2 + 4\alpha\gamma)p_1 + 4\alpha\beta p_0)xy \\ &\quad + (4\gamma^2 p_2 - 2\beta\gamma p_1 + \beta^2 p_0)y^2. \end{aligned}$$

Hence, we have  $\tau = -1$  if and only if  $(p_2, p_1, p_0)^T$  is in the null space of the matrix

$$\begin{pmatrix} 4\alpha\gamma & -2\alpha\beta & 4\alpha^2 \\ 4\beta\gamma & -2\beta^2 & 4\alpha\beta \\ 4\gamma^2 & -2\beta\gamma & 4\alpha\gamma \end{pmatrix} \sim \begin{pmatrix} 2\gamma & -\beta & 2\alpha \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Here, we used the fact that  $\alpha > 0$ , and so the second and the third rows of the matrix on the left are scalar multiples of the first row. This show that  $\tau = -1$  is equivalent to  $p_0 = (\beta p_1 - 2\gamma p_2)/(2\alpha)$ . Similarly, we have  $\tau = 1$  if and only if  $(p_2, p_1, p_0)^T$  lies in the null space of the matrix

$$\begin{pmatrix} -4\alpha\gamma + 2\beta^2 & -2\alpha\beta & 4\alpha^2 \\ 4\beta\gamma & -8\alpha\gamma & 4\alpha\beta \\ 4\gamma^2 & -2\beta\gamma & -4\alpha\gamma + 2\beta^2 \end{pmatrix} \sim \begin{pmatrix} -2\alpha\gamma + \beta^2 & -\alpha\beta & 2\alpha^2 \\ \beta\gamma & -2\alpha\gamma & \alpha\beta \\ 0 & 0 & 0 \end{pmatrix}.$$

The row reduction follows because in the matrix on the left, the third row is the sum of  $-\gamma/\alpha$  times the first row and  $\beta/(2\alpha)$  times the second row. But the matrix on the right further row reduces to

$$\begin{pmatrix} \gamma & 0 & -\alpha \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} \beta & -\alpha & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \gamma & 0 & -\alpha \\ 0 & \gamma & -\beta \\ 0 & 0 & 0 \end{pmatrix},$$

respectively, when  $\beta = 0$ ,  $\gamma = 0$ , and  $\beta, \gamma \neq 0$ . From here, we easily see that  $\tau = 1$  is equivalent to  $p = (p_2/\alpha)f$ , as claimed.  $\square$

Lemmas 8.1 and 8.2 have the following consequence.

**Lemma 8.3.** *For any reducible  $F \in V_{\mathbb{Z},f}^0$ , we have  $F = pq$  for some  $p, q \in W_{\mathbb{Z}}$ .*

*Proof.* Let  $F \in V_{\mathbb{Z},f}^0$  be a reducible form, and suppose that  $F$  is not a product of two quadratic forms over  $\mathbb{Z}$ . Then, by Gauss's lemma, this means that  $F$  is not a product of two quadratic forms over  $\mathbb{Q}$  and so has exactly one linear factor over  $\mathbb{Q}$ , say  $\ell(x, y)$ .

Observe that  $\sqrt{-\mathcal{D}} \cdot \ell_{M_f}$  is also a linear factor of  $F$  over  $\mathbb{Q}$  because  $F_{M_f} = F$ , and so it must be proportional to  $\ell$  over  $\mathbb{Q}^\times$ . Since  $\ell$  has coefficients in  $\mathbb{Q}$ , we then deduce from (8.1) in Lemma 8.1 that  $\mathcal{D}$  is a square in  $\mathbb{Z}$ . Put  $G(x, y) = F(x, y)/\ell(x, y)$  and

$$G(x, y) = g_1(x, y)g_2(x, y)g_3(x, y),$$

where each  $g_i(x, y)$  is a linear form over  $\mathbb{C}$ . Observe that  $g_1, g_2, g_3$  are pairwise non-proportional over  $\mathbb{C}^\times$  because  $\Delta(F) \neq 0$ . But  $G_{M_f}$  and  $G$  are proportional over  $\mathbb{C}^\times$  because  $\ell_{M_f}$  and  $\ell$  are. Hence, there is a permutation  $\sigma$  on  $\{1, 2, 3\}$  such that  $(g_i)_{M_f}$  is proportional to  $g_{\sigma(i)}$  over  $\mathbb{C}^\times$  for each  $i \in \{1, 2, 3\}$ , and it must have order dividing two because  $(M_f)^2 = \mathcal{D}I_{2 \times 2}$  fixes each  $g_i$  up to sign. It follows that  $(g_i)_{M_f}$  is proportional to  $g_i$  over  $\mathbb{C}^\times$  for at least one  $i \in \{1, 2, 3\}$ . But  $\mathcal{D}$  is a square in  $\mathbb{Z}$ , and again by (8.1) in Lemma 8.1, we deduce that  $g_i$  is proportional over  $\mathbb{C}^\times$  to a form with coefficients in  $\mathbb{Q}$ . This contradicts that  $\ell$  is the only linear factor of  $F$  over  $\mathbb{Q}$ .  $\square$

**Proposition 8.4.** *For any reducible  $F \in V_{\mathbb{Z},f}^0$ , one of the following holds.*

- (1) *There exists  $p \in W_{\mathbb{Z}}$  and  $m \in \mathbb{Q}^\times$  such that  $F = m \cdot pp_{M_f}$ .*
- (2) *There exist  $p, q \in W_{\mathbb{Z}}$  such that  $p_{M_f} = -p$  and  $q_{M_f} = -q$ .*

*Proof.* First, we show that there exist  $p, q \in W_{\mathbb{Z}}$  such that  $F = pq$ , and

$$(8.2) \quad p_{M_f} = \tau \cdot q \text{ or } p_{M_f} = \tau \cdot p$$

for some  $\tau \in \mathbb{Q}^\times$ . If  $F = pq$  for some irreducible forms  $p, q \in W_{\mathbb{Z}}$ , then note that  $p_{M_f}$  and  $q_{M_f}$  have coefficients in  $\mathbb{Q}$ . Since  $F = F_{M_f}$ , we have  $pq = p_{M_f}q_{M_f}$ , and it is clear that (8.2) holds for some  $\tau \in \mathbb{Q}^\times$ . If  $F$  is not a product of any two irreducible forms in  $W_{\mathbb{Z}}$ , then by Lemma 8.3, we have

$$F(x, y) = g_1(x, y)g_2(x, y)g_3(x, y)g_4(x, y),$$

where each  $g_i(x, y)$  is a linear form over  $\mathbb{Z}$ . Notice that  $g_1, g_2, g_3, g_4$  are pairwise non-proportional over  $\mathbb{C}^\times$  because  $\Delta(F) \neq 0$ . Since  $F = F_{M_f}$ , there exists a permutation  $\sigma$  on  $\{1, 2, 3, 4\}$  such that  $(g_i)_{M_f}$  is proportional to  $g_{\sigma(i)}$  for each  $i \in \{1, 2, 3, 4\}$ , and it must have order dividing two because  $(M_f)^2 = \mathcal{D}I_{2 \times 2}$  fixes each  $g_i$  up to sign. Then, by renumbering if necessarily, we may assume that

$$\sigma = \in \{(1)(2)(3)(4), (1)(2)(34), (12)(34)\}.$$

Taking  $p = g_1g_2$  and  $q = g_3g_4$ , we see that  $p_{M_f} = \tau \cdot p$  holds for some  $\tau \in \mathbb{Q}^\times$ .

Now, by the above, we may write  $F = pq$  for some  $p, q \in W_{\mathbb{Z}}$  such that (8.2) holds for some  $\tau \in \mathbb{Q}^\times$ . If  $p_{M_f} = \tau \cdot q$ , then  $F = m \cdot pp_{M_f}$ , where  $m = 1/\tau$ , and (1) holds. If  $p_{M_f} = \tau \cdot p$ , then  $\tau = \pm 1$  by Lemma 8.2, and also  $q_{M_f} = \tau \cdot q$  since  $pq = p_{M_f}q_{M_f}$ . Note that  $\tau \neq 1$ , for otherwise  $F = uf^2$  for some  $u \in \mathbb{Q}^\times$  by Lemma 8.2, which contradicts that  $\Delta(F) \neq 0$ . Hence, we have (2) in this case. This completes the proof.  $\square$

Given a reducible form  $F \in V_{\mathbb{Z},f}^0$ , we shall say that it is of *type 1* if (1) in Proposition 8.4 holds, and of *type 2* if (2) in Proposition 8.4 holds.

**8.2. Reducible forms of type 1.** By Proposition 8.5 below, and Theorems 1.2, 1.3, and 1.4 (b), we see that it suffices to count the reducible forms in  $V_{\mathbb{Z},f}^0$  of type 2.

**Proposition 8.5.** *Any reducible  $F \in V_{\mathbb{Z},f}^0$  of type 1 has square discriminant in  $\mathbb{Z}$ .*

*Proof.* Let  $F \in V_{\mathbb{Z},f}^0$  be a reducible form of type 1, say  $F = m \cdot pp_{M_f}$ , where  $m \in \mathbb{Q}^\times$  and  $p \in W_{\mathbb{Z}}$ . By (1.4) and Proposition 3.5, we know that  $(L_f(F)^2 + 4K_f(F))/9 \in \mathbb{Z}$ , and that  $\Delta(F)$  is a square if and only if  $(L_f(F)^2 + 4K_f(F))/9$  is a square. Write

$$p(x, y) = p_2x^2 + p_1xy + p_0y^2.$$

Using Proposition 3.6, we compute that  $(L_f(F)^2 + 4K_f(F))/9$  is equal to

$$\left( \frac{4m(\alpha^2p_0^2 - \alpha\beta p_0p_1 + \alpha\gamma p_1^2 + \beta^2p_0p_2 - 2\alpha\gamma p_0p_2 - \beta\gamma p_1p_2 + \gamma^2p_2^2)}{\mathcal{D}} \right)^2,$$

where  $\mathcal{D}$  is the discriminant of  $f$ . This is a square in  $\mathbb{Q}$  and hence a square in  $\mathbb{Z}$ .  $\square$

**8.3. Reducible forms of type 2.** Let  $F \in V_{\mathbb{Z},f}^0(X)$  be a reducible form of type 2. Then, we have  $F = pq$  for some  $p, q \in W_{\mathbb{Z}}$  with  $p_{M_f} = -p$  and  $q_{M_f} = -q$ . Write

$$p(x, y) = p_2x^2 + p_1xy + p_0y^2 \text{ and } q(x, y) = q_2x^2 + q_1xy + q_0y^2,$$

where  $p_0 = (\beta p_1 - 2\gamma p_2)/(2\alpha)$  and  $q_0 = (\beta q_1 - 2\gamma q_2)/(2\alpha)$  by Lemma 8.2. So then

$$F(x, y) = (p_2q_2)x^4 + (p_2q_1 + p_1q_2)x^3y + (p_2q_0 + p_1q_1 + p_0q_2)x^2y^2 + (*)xy^3 + (*)y^4,$$

and we have

$$(8.3) \quad p_2q_0 + p_1q_1 + p_0q_2 = -\frac{2\gamma}{\alpha}p_2q_2 + \frac{\beta}{2\alpha}(p_2q_1 + p_1q_2) + p_1q_1.$$

An explicit computation using Proposition 3.6 then yields

$$\frac{L_f(F)^2 + 4K_f(F)}{9} = \frac{\alpha p_1^2 - 2\beta p_1p_2 + 4\gamma p_2^2}{\alpha} \cdot \frac{\alpha q_1^2 - 2\beta q_1q_2 + 4\gamma q_2^2}{\alpha},$$

which is non-zero by (1.4). Also, since  $p_0, q_0 \in \mathbb{Z}$ , both of the quotients on the right are integers. We then deduce that

$$(8.4) \quad |(\alpha p_1^2 - 2\beta p_1p_2 + 4\gamma p_2^2)/\alpha|, |(\alpha q_1^2 - 2\beta q_1q_2 + 4\gamma q_2^2)/\alpha| \geq 1.$$

Since  $\max\{L_f(F)^2, |K_f(F)|\} \leq X$ , we also have

$$(8.5) \quad |(\alpha p_1^2 - 2\beta p_1p_2 + 4\gamma p_2^2)/\alpha| |(\alpha q_1^2 - 2\beta q_1q_2 + 4\gamma q_2^2)/\alpha| \leq X.$$

If  $f$  is positive definite or reducible, then (8.4) and (8.5) will suffice. If  $f$  is indefinite and irreducible, then we note that there exists  $t \in \mathbb{R}$  depending only on  $F$  such that

$$p_2q_2, p_2q_1 + p_1q_2, p_2q_0 + p_1q_1 + p_0q_2 = O_f(X^{1/2} + X^{1/2} \cosh(4t) + X^{1/2} \sinh(4t))$$

by the parametrization of  $V_{\mathbb{R},f}^0$  given by (4.11) and Proposition 5.6, and the formulae in (5.12) and (5.13). But as shown in the proof of Theorem 1.4 (a), up to the  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence class of  $F$ , we may take  $t \in [0, t_D]$ , where  $t_D$  is defined as in (1.9). This, together with (8.3), then implies that there exists a constant  $\mathcal{B}'_f$  depending only on  $f$  such that we may take  $p_2, p_1, q_2, q_1$  to satisfy

$$(8.6) \quad |p_2q_2|, |p_2q_1 + p_1q_2|, |p_1q_1| \leq \mathcal{B}'_f X^{1/2}.$$

If  $f$  is positive definite or reducible, then we simply define  $\mathcal{B}'_f = \infty$ . Since  $p_2, p_1, q_2, q_1$  are integers, for convenience we shall also impose that

$$(8.7) \quad |p_2|, |\alpha p_1 - \beta p_2|, |q_2|, |\alpha q_1 - \beta q_2| \geq 1.$$

We are now ready to prove Theorems 1.2, 1.3, and 1.4 (c).

To that end, let  $N_{\mathbb{Z},f}^{\mathrm{red},2}(X)$  denote the number of  $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of the reducible forms in  $V_{\mathbb{Z},f}^0(X)$  of type 2. Then, it suffices to show that

$$(8.8) \quad N_{\mathbb{Z},f}^{\mathrm{red},2}(X) = \begin{cases} O_f(X(\log X)^3) & \text{if } f \text{ is reducible} \\ O_f(X(\log X)^2) & \text{if } f \text{ is irreducible} \end{cases}$$

by Proposition 8.5, as well as Theorems 1.2, 1.3, and 1.4 (b). By the above discussion, we know that  $N_{\mathbb{Z},f}^{\mathrm{red},2}(X)$  is bounded above by the number of integral points in

$$\mathcal{R}'_f(X) = \{(p_2, p_1, q_2, q_1) \in \mathbb{R}^4 \mid (8.4), (8.5), (8.6), (8.7)\}.$$

Let  $D = |\mathcal{D}|$ , where  $\mathcal{D}$  denotes the discriminant of  $f$ . In view of the relation

$$(\alpha x^2 - 2\beta xy + 4\gamma y^2)/\alpha = ((\alpha x - \beta y)^2 - \mathcal{D}y^2)/\alpha^2,$$

we shall make the change of variables

$$\Xi_f : \mathbb{R}^4 \longrightarrow \mathbb{R}^4; \quad \Xi_f(p_2, p_1, q_2, q_1) = (u_2, u_1, v_2, v_1)$$

by setting

$$u_2 = \sqrt{D}p_2, \quad u_1 = \alpha p_1 - \beta p_2, \quad v_2 = \sqrt{D}q_2, \quad v_1 = \alpha q_1 - \beta q_2.$$

The conditions (8.4) and (8.5) may then be rewritten as

$$(8.9) \quad \begin{cases} |u_1^2 + u_2^2|, |v_1^2 + v_2^2| \geq \alpha^2, |u_1^2 + u_2^2||v_1^2 + v_2^2| \leq \alpha^4 X & \text{if } f \text{ is positive definite} \\ |u_1^2 - u_2^2|, |v_1^2 - v_2^2| \geq \alpha^2, |u_1^2 - u_2^2||v_1^2 - v_2^2| \leq \alpha^4 X & \text{if } f \text{ is indefinite.} \end{cases}$$

Also, the conditions (8.6) and (8.7) imply that

$$(8.10) \quad |u_2|, |u_1|, |v_2|, |v_1| \geq 1, |u_2 v_2| \leq D \mathcal{B}'_f X^{1/2}, |u_1 v_1| \leq (\alpha + |\beta|)^2 \mathcal{B}'_f X^{1/2}$$

We shall treat the cases when  $f$  is reducible and when  $f$  is irreducible separately.

**8.4. Proof of Theorem 1.3 (c).** Suppose that  $f$  is reducible, in which case  $D$  is a square in  $\mathbb{Z}$ . As noted, it suffices to show (8.8), and the quantity  $N_{\mathbb{Z},f}^{\text{red},2}(X)$  is bounded above by the number of integral points in  $\mathcal{R}'_f(X)$ .

We shall further make the change of variables

$$\Xi'_f : \mathbb{R}^4 \longrightarrow \mathbb{R}^4; \quad \Xi'_f(u_2, u_1, v_2, v_1) = (z_1, z_2, z_3, z_4)$$

by setting

$$z_1 = u_1 + u_2, z_2 = u_1 - u_2, z_3 = v_1 + v_2, z_4 = v_1 - v_2.$$

Since  $D$  is a square in  $\mathbb{Z}$ , the matrix of  $\Xi'_f \circ \Xi_f$  has entries in  $\mathbb{Z}$ . Hence, the number of integral points in  $\mathcal{R}'_f(X)$  is bounded above by that in  $(\Xi'_f \circ \Xi_f)(\mathcal{R}'_f(X))$ . By (8.9), the integral points of  $(\Xi'_f \circ \Xi_f)(\mathcal{R}'_f(X))$  in turn are contained in

$$\mathcal{S}'_f(X) = \{(z_1, z_2, z_3, z_4) \in \mathbb{R}^4 \mid |z_1|, |z_2|, |z_3|, |z_4| \geq 1 \text{ and } |z_1 z_2 z_3 z_4| \leq \alpha^4 X\},$$

which is clearly a semi-algebraic subset of  $\mathbb{R}^4$ . Applying Proposition 4.1, we obtain

$$N_{\mathbb{Z},f}^{\text{red},2}(X) \leq \text{Vol}(\mathcal{S}'_f(X)) + O(\max\{\text{Vol}(\overline{\mathcal{S}'_f(X)}), 1\}).$$

We easily see that

$$\begin{aligned} \text{Vol}(\mathcal{S}'_f(X)) &= 16 \int_1^{\alpha^4 X} \int_1^{\alpha^4 X/z_4} \int_1^{\alpha^4 X/(z_3 z_4)} \int_1^{\alpha^4 X/(z_2 z_3 z_4)} dz_1 dz_2 dz_3 dz_4 \\ &= O_f(X(\log X)^3). \end{aligned}$$

Since each coordinate is bounded by  $O_f(X)$ , the 1-dimensional projections of  $\mathcal{S}'_f(X)$  have lengths  $O_f(X)$ . The volume of the projection by equating  $z_1$  and  $z_2$  to zero is

$$4 \int_1^{\alpha^4 X} \int_1^{\alpha^4 X/z_4} dz_3 dz_4 = O_f(X \log X).$$

Similarly, the volume of the projection by equating  $z_1$  to zero is

$$8 \int_1^{\alpha^4 X} \int_1^{\alpha^4 X/z_4} \int_1^{\alpha^4 X/(z_3 z_4)} dz_2 dz_3 dz_4 = O_f(X(\log X)^2).$$

By symmetry, this shows that the 2- and 3-dimensional projections of  $\mathcal{S}'_f(X)$ , respectively, all have volumes bounded by  $O_f(X \log X)$  and  $O_f(X(\log X)^2)$ . The claim (8.8) now follows.



**8.5. Proof of Theorems 1.2 and 1.4 (c).** Suppose that  $f$  is irreducible. By the discussion in Section 8.3, it suffices to show (8.8), and  $N_{\mathbb{Z},f}^{\text{red},2}(X)$  is bounded above by the number of integral points in  $\mathcal{R}'_f(X)$ .

It is clear that  $\mathcal{R}'_f(X)$  is a semi-algebraic subset of  $\mathbb{R}^4$ . Applying Proposition 4.1, we then obtain

$$N_{\mathbb{Z},f}^{\text{red},2}(X) \leq \text{Vol}(\mathcal{R}'_f(X)) + O(\max\{\text{Vol}(\overline{\mathcal{R}'_f(X)}), 1\}).$$

Put  $\mathcal{S}'_f(X) = \Xi_f(\mathcal{R}'_f(X))$ , and observe that

$$\text{Vol}(\mathcal{R}'_f(X)) = O_f(\mathcal{S}'_f(X)) \text{ and } \text{Vol}(\overline{\mathcal{R}'_f(X)}) = O_f(\text{Vol}(\overline{\mathcal{S}'_f(X)}))$$

since the linear transformation  $\Xi_f$  depends only on  $f$ . Also, put

$$\mathcal{B}_f^* = \begin{cases} \alpha^2 & \text{if } f \text{ is positive definite} \\ \max\{D, (\alpha + |\beta|)^2\} \mathcal{B}'_f & \text{if } f \text{ is indefinite.} \end{cases}$$

We easily deduce from (8.9) and (8.10) that the points  $(u_2, u_1, v_2, v_1) \in \mathcal{S}'_f(X)$  satisfy

$$1 \leq |u_2|, |u_1|, |v_2|, |v_1| \leq (\mathcal{B}_f^* X)^{1/2} \text{ and } |u_2 v_2|, |u_1 v_1| \leq \mathcal{B}_f^* X^{1/2}.$$

It follows that  $\text{Vol}(\mathcal{S}'_f(X))$  is bounded above by

$$16 \left( \int_1^{(\mathcal{B}_f^* X)^{1/2}} \int_1^{\mathcal{B}_f^* X^{1/2}/v_2} du_2 dv_2 \right) \left( \int_1^{(\mathcal{B}_f^* X)^{1/2}} \int_1^{\mathcal{B}_f^* X^{1/2}/v_1} du_1 dv_1 \right) = O_f(X(\log X)^2).$$

Now, since each coordinate is bounded by  $O_f(X^{1/2})$ , it is clear that the 1-dimensional and 2-dimensional projections of  $\mathcal{S}'_f(X)$  have lengths equal to  $O_f(X^{1/2})$  and  $O_f(X)$ , respectively. The volume of the projection by equating  $u_2$  to zero is at most

$$8 \int_1^{(\mathcal{B}_f^* X)^{1/2}} \int_1^{(\mathcal{B}_f^* X)^{1/2}} \int_1^{\mathcal{B}_f^* X^{1/2}/v_1} du_1 dv_1 dv_2 = O_f(X \log X).$$

By symmetry, we deduce that the volumes of the 3-dimensional projections of  $\mathcal{S}'_f(X)$  are all bounded by  $O_f(X \log X)$ , whence  $\text{Vol}(\overline{\mathcal{S}'_f(X)}) = O_f(X \log X)$ . From this, we see that (8.8) indeed holds, and this proves the claim.

## REFERENCES

- [1] M. A. Bean, *The practical computation of areas associated with binary quartic forms*, Math. Comp. (66) **219** (1997), 1269-1293.
- [2] M. Bhargava, A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. **181** (2015), 191-242.
- [3] M. Bhargava, A. Shankar, J. Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, Invent. math. **193** (2013), 193-439
- [4] M. Bhargava, A. Shnidman, *On the number of cubic orders of bounded discriminant having automorphism group  $C_3$ , and related problems*, Algebra and Number Theory (1) **8** (2014), 53-88.
- [5] J. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2** (1999), 64-94.
- [6] H. Davenport, *On the class-number of binary cubic forms, I*, J. London Math. Soc. **26** (1951), 183-192.
- [7] H. Davenport, *On the class-number of binary cubic forms II*, J. Lond. Math. Soc. **26**, (1951) 192-198,
- [8] L. E. Dickson, *History of the Theory of Numbers*, Carnegie Institution of Washington (1919), pg 116.
- [9] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), 1973, 91-101.
- [10] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.
- [11] M. Newman, *Integral matrices*, Pure and Appl. Math. (S. Eilenberg and P. A. Smith, eds.), vol. 45, Academic Press, New York, 1972.
- [12] S. Ramanujan, *Some formulae in the analytic theory of numbers*, Messenger of Math. **45** (1916), 81-84.
- [13] C. L. Siegel, *The average measure of quadratic forms with given determinant and signature*, Annals of Mathematics (4) **45** (1944), 667-685.
- [14] T. Taniguchi, F. Thorne, *Secondary terms in counting functions for cubic fields*, Duke Math. J., (13) **162** (2013), 2451-2508.
- [15] B.M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, Proc. London Math. Soc. (2) **21** (1922), 235-255.
- [16] S. Y. Xiao, *On binary cubic and quartic forms*, arXiv:1610.09208 [math.NT].
- [17] D. J. Zywina, *Hilbert's irreducibility theorem and the larger sieve*, arXiv:1011.6465 [math.NT].

YAU MATHEMATICAL SCIENCES CENTER, TSINGHUA UNIVERSITY, BEIJING 100084, P.R. CHINA

*E-mail address:* sinyitsang@math.tsinghua.edu.cn

MATHEMATICAL INSTITUTE, UNIVERSITY OF OXFORD, OXFORD, OX2 6GG, UNITED KINGDOM

*E-mail address:* y28xiao@uwaterloo.ca